DOCUMENT RESUME

ED 166 631	CG 013 246

AUTHOR	Trubow, George B.
TITLE	Privacy and Security of Criminal History Information: An Analysis of Privacy Issues.
SPONS AGENCY	National Criminal Justice Information and Statistics Service (Dept. of Justice/LEAA), Washington, D.C.
PUB DATE	78
CONTRACT	LEAA-7-0553-J-LEAA
NOTE	83p.; Parts may be marginally legible due to print quality
AVAILABLE FROM	Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402 (027-000-00712-1)
EDRS PRICE	MF-$0.83 HC-$4.67 Plus Postage.
DESCRIPTORS	Civil Rights; *Criminal Law; Criminals; *Information Storage; *Information Utilization; *Justice; *Policy Formation; *Privacy; Program Development; Security (Psychology); State Legislation

ABSTRACT

Policies and issues associated with the privacy and security of criminal history information are presented. The first chapter discusses general concepts regarding privacy and security of criminal justice information, including definitions of basic terms, considerations of interests requiring attention when developing policy, relevance of fair information practices, and constraints of system design. The second chapter provides information regarding specific issues in developing privacy policy such as costs, public record laws, state and federal regulatory authority, types of information, and access. The third chapter describes the criminal justice information privacy and security programs in the states of Colorado, Illinois, Maryland, and Washington, as well as providing suggestions for developing these programs. (Author/HLM)

****
* Reproductions supplied by EDRS are the best that can be made *
* from the original document. *
****

ED166631

U.S. DEPARTMENT OF HEALTH,
EDUCATION & WELFARE
NATIONAL INSTITUTE OF
EDUCATION

THIS DOCUMENT HAS BEEN REPRODUCED EXACTLY AS RECEIVED FROM THE PERSON OR ORGANIZATION ORIGINATING IT. POINTS OF VIEW OR OPINIONS STATED DO NOT NECESSARILY REPRESENT OFFICIAL NATIONAL INSTITUTE OF EDUCATION POSITION OR POLICY.

U.S. Department of Justice
Law Enforcement Assistance Administration

James M.H. Gregg
Acting Administrator

Harry Bratt
Assistant Administrator
National Criminal Justice Information
 and Statistics Service

Carol G. Kaplan
Director, Privacy and Security Staff

Document prepared by George B. Trubow pursuant to LEAA Contract 7-0553-J-LEAA.

Contents of the document do not necessarily reflect the views or policies of the Law Enforcement Assistance Administration or the Department of Justice.

Privacy and Security of Criminal History Information

AN ANALYSIS OF PRIVACY ISSUES

National Criminal Justice Information and Statistics Service
Law Enforcement Assistance Administration
U.S. Department of Justice

1978

ACKNOWLEDGMENTS

This report on the dissemination of criminal justice information was prepared as the principal task of a project under the auspices of the National Criminal Justice Information and Statistics Service of the Law Enforcement Assistance Administration, United States Department of Justice. Views expressed herein are mine and do not necessarily reflect the position of NCJISS or LEAA.

Though I am at fault for any shortcomings in the report, I acknowledge the splendid cooperation of many state and local officials, criminal justice personnel and citizens who helped me with the materials and insights. Especial thanks go to Gary Pon of Colorado, Paul Fields of Illinois, Michel Lettre of Maryland, and Thomas Dalton of Washington State, who were extremely helpful in pointing me to sources of information regarding their respective state's program.

Emanuel Krakauer, and Judith Gilliland, senior research assistants, helped in the preparation of this document, and I appreciate it. Thanks for faithful secretarial assistance go to Diane Gordon, whose spirit of cooperation never flagged.

Throughout this effort, Carol Kaplan, Director of the NCJISS Privacy Staff, provided encouragement and sound advice, and exhibited an extreme measure of patience, for all of which I am especially grateful.

George B. Trubow
The John Marshall Law School
Chicago, Illinois

For sale by the Superintendent of Documents, U.S. Government Printing Office
Washington, D.C. 20402

Stock No. 027-000-00712-1

TABLE OF CONTENTS

Introduction 1

Chapter I. General Privacy Considerations 4

- Definition of Terms 5
  - Access 5
  - Criminal History Record Information 5
  - Criminal Justice Agency 5
  - Criminal Justice Administration 5
  - Criminal Justice Information 5
  - Disposition 5
  - Dissemination 6
  - Intelligence & Investigative Information 6
  - Non-Conviction Data 6
  - Purge 6
  - Seal 6
- Interests Affecting Confidentiality 7
  - The Individual 7
  - The Criminal Justice System 7
  - Society At Large 8
- Fair Information Practices
  - No Secret System 9
  - Data Subject Access 10
  - Data Subject Challenge 10
  - Restrict Data Use 10
  - Use Valid Data 11
  - Safeguard the Data 11
- Legal Constraints on Information Use 12
  - Federal Legislation 12
  - Federal Case Law 12
  - State Case Law 13
- Information System Configuration 14
  - Manual v. Automated 14
  - Centralized v. De-Centralized 14
  - Dedicated v. Non-Dedicated Systems 14

Chapter II. Specific Issues of Privacy 16

- Privacy Costs 16
- State Regulatory Authority 16
- Privacy and Security Council 17
- Relevance of Public Records Laws 17
- Regulation of Dissemination 19
  - Arrest Information 19
  - Non-Conviction Data 20
  - Investigative & Intelligence Information 20
  - Conviction Information 21
  - Government vs. Private Sector Access 22
- Access By Data Subject 24
- Right to Challenge 24
- Judicial Review of Challenge 24
- Purging or Sealing 25
- Removal of Disqualifications 26
- Right to State Non-Existence of Record 26
- Researcher Access 26
- Accuracy and Completeness 27
- Civil Remedies 27
- Criminal Penalties 27
- Separation of Files 28
- Regulation of Intelligence Collection 28
- Regulation of Intelligence Dissemination 28
- Security 29
- Transaction Logs 29
- Training of Employees 29
- Listing of Information Systems 30

Chapter III. Examples of State Programs 31

- o Colorado 32
  - . Colorado Criminal Justice System 32
  - . Criminal Justice Information System 32
  - . Development of the State's Privacy Program 33
  - . Significant Issues 35
  - . Some Remaining Problems 36
  - . Words From The Wise 36
- o Illinois 43
  - . Illinois Criminal Justice System 43
  - . Criminal Justice Information System 44
  - . Development of the State's Privacy Program 44
  - . Individual Review and Challenge 46
  - . Some Remaining Problems 46
- o Maryland 51
  - . Maryland Criminal Justice System 51
  - . Criminal Justice Information System 52
  - . Development of the State's Privacy Program 53
  - . Dissemination Policy 54
  - . Issues For The Future 56
  - . A Comment On Process 56

- o Washington State

  - . Washington Criminal Justice System 64
  - . Criminal Justice Information System 64
  - . Development of the State's Privacy Program 65
  - . Dissemination Policy 66
  - . Other Laws Affecting Information 67
  - . Public Records Law 67
  - . State Human Rights Commission Regs 68
  - . Issues For The Future 68
- o Some Points On Process 70

Footnotes 72

ABBREVIATED REFERENCES

Comprehensive Data System	CDS
Computerized Criminal History	CCH
Criminal Justice Information	CJI
Criminal Justice Information System	CJIS
Intelligence and Investigative Information	I&I
Law Enforcement Assistance Administration, U.S. Department of Justice	LEAA
National Advisory Commission on Criminal Justice Standards and Goals	NAC
Offender Based State Correction Information System	OBSCIS
Offender Based Transaction System	OBTS
SEARCH Group, Inc.; Project SEARCH	SGI
State Criminal Justice Planning Agency	SPA
Title 28 CFR, Part 20	Title 28
National Criminal Justice Information and Statistics Service	NCJISS

INTRODUCTION

"Privacy" has gained attention of late in every area of personal affairs. Of singular importance has been the subject of "privacy and security" of criminal justice information. Often the desires for anonymity by those who have confronted the criminal justice system clash with society's inquiries pursuant to a "right to know."

The enactment of the Omnibus Crime Control and Safe Streets Act of 1968, brought national attention to state criminal justice systems, and Federal funding through the newly established Law Enforcement Assistance Administration. A significant LEAA priority was the development of comprehensive criminal justice information; and the encouragement of states in the development or upgrading of such information systems.

In early 1973, the National Advisory Commission on Criminal Justice Standards and Goals, mindful of information system development, encouraged each state to

> ". . . adopt enabling legislation for protection of security and privacy in criminal justice information systems. The enabling statute should establish an administrative structure, minimum standards for protection of security and privacy, and civil and criminal sanction for violation of statutes or rules and regulations adopted under it."

The NAC also recommended that each state establish a security and privacy council to oversee and monitor criminal justice information privacy programs; training for criminal justice personnel regarding privacy and security measures also was recommended. 1/

A few months after the NAC report, the Crime Control Act of 1973 amended the earlier 1968 Act, and required that information systems developed with Federal funds be protected by measures to insure the privacy and security of criminal justice information. 2/ Section 524(b) of the 1973 Act provides as follows:

> "All criminal history information collected, stored or disseminated through support under this title shall contain, to the maximum extent feasible, disposition as well as arrest data where arrest data is included therein. The collection, storage and dissemination of such information shall take place under procedures reasonably designed to insure that all such information is kept current therein; the administration shall assure that the security and privacy of all information is adequately provided for and that information shall only be used for law enforcement and criminal justice

> and other lawful purposes. In addition, an individual who believes that criminal history information concerning him contained in an automated system is inaccurate, incomplete, or maintained in violation of this title, shall, upon satisfactory verification of his identity, be entitled to review such information and to obtain a copy of it for the purpose of challenge or correction."

Pursuant to mandate in the foregoing legislation, LEAA developed regulations which were initially published in May, 1975, revised and finally promulgated in March, 1976, and which appear in Title 28 of the Code of Federal Regulations, Chapter 1, Part 20. These regulations impose requirements with respect to the dissemination of criminal history record information, though mainly the regulations leave it to the states to develop comprehensive programs to manage criminal justice information.

This report was prepared as one of the tasks in a project undertaken for the National Criminal Justice Information and Statistic Service (NCJISS) of the Law Enforcement Assistance Administration, United States Department of Justice. A specific purpose of the project was to survey state legislation dealing with limitations on the dissemination of criminal history information. The results of that survey are included in a companion document, "Privacy and Security of Criminal History Information: A Compendium of State Statutes," available from NCJISS.

In broader perspective, the project was intended to analyze privacy policy and to produce a resource document that would be of help to state and local government for the development of privacy and security programs in criminal justice information systems. This project does not address the special complexities of juvenile justice information, though many of the policy issues are the same.

It is not the purpose of this report to advocate a particular framework for legislative policy or a "model" statute for state government. The Compendium of legislative approaches to particular policy choices should be a useful resource to those concerned with legislative policy and drafting. This report will discuss matters contemplated within 28 CFR, Part 20, and will explore a broader range of privacy and security issues that a state may confront in developing a comprehensive program. 3/

The organization of this monograph is quite simple. Chapter I is a discussion of the general concepts regarding privacy and security with respect to criminal justice information, including a definition of some basic terms, consideration of the interests to be balanced in developing privacy policy, the relevance of fair information practices, and the constraints of system design.

Chapter II contains a discussion of specific issues to be resolved in developing privacy policy for criminal justice information systems. These issues are presented more as a list of options than as guidelines for adoption, and the choices available to policy makers are identified.

Chapter III presents the criminal justice information privacy and security program developed in each of four states: Colorado, Illinois, Maryland and Washington. These states are cited as examples of legislative programs that should be of interest to those who intend to undertake, review or reshape their own criminal justice information privacy policy.

At the end of Chapter III there are brief suggestions for how to deal with the development of a criminal justice information privacy program. Frequently the process for developing policy is just as important as the substance.

CHAPTER I. GENERAL CONSIDERATIONS FOR PRIVACY AND SECURITY OF CRIMINAL JUSTICE INFORMATION.

The phrase, "privacy and security" is in general use today, not only as to criminal justice information, but with respect to any kind of personal information, i.e., any information that is referenced to an identifiable individual by use of name, number or other characteristic. That which makes information personal is not its content, but whether it refers to a specific individual. Criminal justice information is one kind of personal information, and is the topic of this report.

The word "privacy" has been used for a broad range of notions such as the right to use contraceptives or to have an abortion, the right not to have one's telephone tapped, and the expectation that one's bank records will not be opened to public scrutiny. In one popular sense, privacy is a desire to be "let alone," and thus it is a concept difficult to define or to limit. Privacy relates to people, and with respect to information about people, raises questions as to what and how information about them is gathered. That inquiry is not the prime focus of this report which instead deals with how information is used.

The term "confidentiality" best describes the subject of this report. We are here concerned with who can have access to specific criminal justice information, and under what circumstances. Confidentiality protects privacy by restricting access to personal information.

The term "security" relates to information systems, and deals with how information is protected from unauthorized access, alteration or loss. Security assures confidentiality and the integrity of data; it is largely the realm of technical experts and will not be treated with here other than by reference.

The phrase "privacy and security," though commonly used, is an unhappy one; it is more useful to talk about personal privacy, data confidentiality, and system security. Though the use of "privacy and security" will be avoided when practicable, it is acknowledged that the phrase is generally accepted as descriptive of policy or rules that relate to limitations on acquisition or use, or the protection of, criminal justice information.

13

Definition of Terms.

To promote clarity in discussion the more important terms used frequently in this report are defined below. Definitions reflect the ordinary meaning of words and the generally accepted use in criminal justice. The main source for the definitions is the SGI glossary, "Security and Privacy Terminology." 4/ In instances where a definition is from LEAA regulations in Title 28, CFR, Part 20, that is indicated by the notation (Regs).

Access. The authority to review or receive information from files, records or an information system, whether manual or automated.

Criminal history record information (CHRI). Information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, information, or other formal criminal charges, and any disposition arising therefrom, sentencing, correctional supervision and release. The term does not include identification information such as fingerprint records to the extent that such information does not indicate involvement of the individual in the criminal justice system. (Regs.)

Criminal justice agency. Any court or other governmental agency or any sub-unit thereof which performs the administration of justice pursuant to a statute or an executive order, and which allocates a substantial part of its budget to the administration of criminal justice. (Regs.)

Criminal justice administration. The performance of any of the following activities: detection, apprehension, detention, pre-trial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. The administration of criminal justice shall include criminal identification activities and the collection, storage and dissemination of criminal history record information. (Regs.)

Criminal justice information (CJI). Information collected by criminal justice agencies that is needed for the performance of their legally authorized and required functions. This is the broadest information term, and includes CHRI and investigative and intelligence information. It does not include agency personnel or administrative records used for agency operations or management.

Disposition. Information disclosing that criminal proceedings have been concluded, including information disclosing that the police have elected not to refer a matter to a prosecutor or that a prosecutor has elected not to commence criminal proceedings and also disclosing the ature of the termination in the proceedings, or information disclosing that proceedings have been indefinitely postponed and also disclosing the reason for such postponement. Disposition shall include, but not be limited to, acquittal, acquittal by reason of insanity, acquittal by reason of mental incompetence, case continued without finding, charge dismissed, charge dismissed due to insanity, charge dismissed due to mental incompetency, charge still pending due to insanity, charge still pending due to mental incompetence, guilty plea nolle prosequi, no paper, nolo contendere plea, convicted, youthful offender determination, deceased, deferred disposition, dismissal-civil action, found insane, found mentally incompetent, pardoned, probation before conviction, sentence commuted, adjudication withheld, mistrial-defendant discharged, executive clemency, placed on probation, paroled, or released from correctional supervision. (Regs.)

Dissemination. The transmission of information, whether orally, in writing or electronically, to anyone outside the agency which maintains the information, except reports to an authorized repository.

Intelligence and investigative information (I&I). Information compiled in an effort to anticipate, prevent or monitor possible criminal activity, or compiled in a course of investigation of known or suspected crimes.

Non-conviction data. Arrest information without disposition if an interval of one year has elapsed from the date of arrest and no active prosecution of the charge is pending; or information disclosing that the police have elected not to refer a matter to a prosecutor, or that a prosecutor has elected not to commence criminal proceedings, or that proceedings have been indefinitely postponed, as well as all acquittals and all dismissals. (Regs.)

Purge. To completely remove from or destroy information contained in a specified file or records system. (The word "expunge," sometimes a synonym for purge, is not used in this report.

Seal. Through special procedures to close or limit access to specified information and files or record systems.

Interests Affecting Criminal Justice
Information Confidentiality.

Policy with respect to the use of criminal justice information must consider the variant, and sometimes competing, interests to be balanced in developing access procedures.

The individual.

The person identified by criminal justice information generally wants to limit access to that data because of its potential for harmful consequences. That perspective itself changes from time to time, however. For example, at the moment of arrest one wants to be sure that family, friends or lawyer can have access to the information; secret arrests are contrary to concepts of a free society and are inconsistent with this nation's constitutional guarantees. Likewise, the accused wants prosecution and trial to be open to scrutiny to deter arbitrary, capricious or discriminatory procedures. An incarcerated offender does not want to "get lost" in the system, or while there to be subjected to improper treatment, and accordingly wants correctional information available to his representatives or to those who monitor the operations of government in the public interest. Once out of the system, however, the individual would like to rewrite history, erasing from its pages any notation of involvement with criminal justice. The mere fact of arrest, though mistaken and followed by the dismissal of charges, is perceived as a blot on one's record that can prevent employment or bring other opprobrium. No matter what the circumstances may have been, however, an individual does not want a criminal record to follow him, and he desires that criminal justice information not be available indefinitely to the public.

The criminal justice system.

The criminal justice system itself cannot function properly without access to CJI. Since it is the system itself which is the main source and principal user of the information, the sharing of CJI by criminal justice agencies is usually appropriate. It is probably safe to say that criminal justice agencies are not much concerned whether the public has access to criminal history record information, except insofar as dissemination may create an administrative burden.

Criminal justice agencies want intelligence and investigative information kept confidential, however, so as not to compromise its value.

Here the interests of the individual and criminal justice coincide, though for differing reasons. The main concern of criminal justice is that dissemination of information not impair the effectiveness of law enforcement.

Society at large.

Prospective employers, especially when the potential employment responsibility is considered "sensitive," want to know about previous criminal justice encounters that job applicants may have had. Often licensing regulations may be conditioned on freedom from criminal history. Those who contemplate important business relations with others (extension of credit, e.g.) also have an interest in criminal history. The relevance of criminal justice information to a particular relationship is enigmatic; a past record may or may not be significant. For instance, public knowledge about a misdemeanor committed during one's youth twenty years past might damage the individual in his relations with others though the value of that stale information is extremely doubtful. Nevertheless, the typical citizen wants access to criminal justice information about others, though he may not want others to have criminal justice information about him.

Policy for criminal justice information access is developed within the context of these interests: fairness to the individual; effectiveness of the criminal justice system; the protection of society. Most policy issues, however, mainly involve a balance between the public's quest for openness and the individual's desire for "privacy."

Fair Information Practices and Criminal Justice.

In fashioning a program for confidentiality of criminal justice information, general principles for good information management should be observed. A personal information system should satisfy the needs of users, but should be managed so as to minimize impairment of the interests of data subjects. A study by an advisory committee to the Secretary of the Department of Health, Education and Welfare resulted in a 1973 report, "Records, Computers and the Rights of Citizens," which examined government practices regarding the use of personal information, and identified ways in which privacy could be enhanced through proper information practice. 5/ The committee recommended "fundamental principles of fair information practice," recognizing that personal privacy is affected by disclosure and use of personal information.

The general principles of the HEW report were incorporated by Congress into the Privacy Act of 1974, and have been accepted generally by the Privacy Protection Study Commission in its 1977 report. 6/ The principles are distilled here as follows:

1. No personal information systems should be maintained whose very existence is secret.

2. A data subject should have access to information about himself and know the purposes for which it is maintained.

3. A data subject should be permitted to challenge and seek corrections of information about himself.

4. Data should be used only for the purposes for which it wa- intended, unless the data subject consents.

5. Information used should be accurate, timely, relevant and complete.

6. Information should be protected against unauthorized access, alteration or destruction.

The following discussion of these general principles flags areas of special implication for criminal justice information.

No secret system.

The Watergate area and its aftermath testify to the utility of

18

this principle in the context of our society and government. Though access to particular information may be restricted for the purposes of state security and other good cause, nevertheless the existence and general purpose of a personal information system should not be a secret. This principle causes no special problem for the criminal justice system and may be accepted without much debate.

Data subject access.

This is a principle of fairness, especially in reference to personal information. Because information is used to make decisions, why not let the data subject see the information used to affect him? The data subject knows what experiences he has had with the system, and there is little reason to deny him access to criminal history records about himself. The main exception to this principle is intelligence and investigative information, to be discussed Chapter II.

Data subject challenge.

In most instances the subject himself is a good resource to check the validity of data in his file. Allowing the subject to see a file without giving him an opportunity to have had data corrected is an incomplete recognition of the individual's interest. The reliability of the contested data can be verified by appropriate data audit procedures.

Restrict data to its intended use.

This principle creates some difficulty for criminal justice in identifying a particular intended use. Information is kept to record official actions of government agencies, to provide the basis for agency actions, to protect the interests of the individual with whom the government is interacting, and to protect the public. As it relates to personal information generally, the principal is acceptable because the data subject usually has voluntarily supplied information about himself for a specific intended use. The information might not have been furnished if some other use were made knwon; to comply with this principle can prevent surprise to the data subject. In most instances, however, criminal justice information is not supplied voluntarily by the data subject, but is required and recorded by law even though it may be against the interest of the data subject. Though the general reason for this principle has less applicability to criminal justice than to other personal information systems, and accordingly may be discounted, it ought not to be discarded without examination. A more detailed discussion of this subject is contained in Chapter II.

Use valid data.

This principle is consistent with good record keeping as well as wth fairness to the individual. The validity of a decision will be impaired if it is based upon data that is wrong, stale or incomplete; the main question for criminal jsutice is what are reasonable standards for accuracy, timeliness and completeness. Some of those standards are suggested in the LEAA regulations, and will be considered in Chapter II.

Safeguard the data.

This principle comports with the interests of the individual, criminal justice, and with sound information management. If data is worth keeping, then it is worth protecting so that its integrity is not impaired nor its confidentiality breached. This principle presents problems in determining what may be considered an acceptable level of security with respect to a particular collection of information, an area wherein there is little guidance at present. Information system managers will have to make subjective judgments regarding security levels appropriate to the particular data to be protected and the probable costs for various levels to protection.

The discussion in Chapter II will consider the foregoing principles, and the competing interests to be balanced, in developing policy for the confidentiality of criminal justice information.

Legal Constraints on Criminal Justice Information Maintenance and Use.

Federal legislation and regulation.

At present the only significant Federal legislative requirements for state criminal justice information use or maintenance are in the Crime Control Act of 1973, previously cited, and the LEAA regulations pursuant thereto in Title 28 CFR, Part 20. Part 22 of Title 28 concerns the use of criminal justice information for research and statistical purposes, and is mentioned in Chapter II. The regulations apply to any state or local criminal justice information system that has received Federal funding, and to those who receive information from such a system.

In brief, 28 CFR, Part 20, requires that non-conviction data be disseminated outside the criminal justice system only pursuant to state law, regulation, executive or court order. The regulations also require some provisions for data subject access and challenge. 8/

The Privacy Act of 1974 applies only to Federal agencies, as does the Federal Freedom of Information Act. Even as to Federal agencies, there are significant exceptions in each of these Acts with respect to criminal justice information, so the LEAA regulations are the principal Federal legislative restraint on state or local criminal justice information systems.

Federal case law.

In the landmark case of Griswold v. Connecticut, the United States Supreme Court articulated the notion of a right of privacy inherent in the U.S. Constitution. 9/ That case, and subsequent decisions, restricted encroachment by government in such personal areas as eavesdropping, use of contraceptives, and the right to abortion. In 1976, however, in the case of Paul v. Davis, the Supreme Court considered a matter involving the dissemination of criminal justice information, and refused to extend the concepts of Federally protected privacy to that subject. 10/ Though state courts are free to define and protect privacy rights with respect to criminal justice information, it appears that the Federal Constitution may not be a basis for such protection.

Though the Federal courts have recognized some limitations on the improper use of criminal justice information, in most instances the uses have involved state, and not Federal, rights. The Attorney General of each state can provide guidance to criminal justice officials. 11/

State case law.

Litigation regarding criminal justice information can be expected at the state level, arising out of common law or state constitutional privacy rights. Common law remedies for defamation protect against the use of inaccurate information, and some courts have allowed sealing of purging of criminal justice information when individual interests were judged to outweigh those of society. There is not much state case law dealing with the subject, and such research is beyond the scope of this project. Again, each state's Attorney General can provide helpful guidance.

Information System Configuration.

The nature and configuration of a particular information system will affect how confidentiality and security is to be implemented, and that is a concern primarily for technical experts. Though not a subject for this report, some questions of system design are noted below.

Manual v. automated.

The requirements of 28 CFR, Part 20, apply to manual and automated criminal justice information systems. It is the choice of state and local government whether to automate, and this decision depends upon the volume of records to be handled and the resources available to purchase and maintain an automated system. Presently the bulk of criminal justice information is maintained manually. Indications are that the use of automated systems will continue to grow at the state level and in large local jurisdictions. Small local jurisdictions may have manual systems even though a central state repository is the agency that disseminates criminal justice information. Information can be kept sufficiently confidential and secure regardless of whether the system in which it is stored is manual or automated.

Centralized v. de-centralized.

Title 28 does not require the states to develop a central repository for criminal justice information, though the language of the regulations contemplates such a repository. From the standpoint of effectiveness and efficiency, it appears that a central repository is the best alternative in most cases. Since the regulations, and good information practice, require that files be complete and current, given the number of agencies that contribute information to criminal histories a decentralized system may entail duplication in effort and might not assure valid information. Operating agencies within the criminal justice system may continue to maintain their own files if they choose. Dissemination from local records should be made in compliance with applicable rules, and a prior inquiry to the central repository will minimize release of invalid data.

Dedicated v. non-dedicated systems.

A basic question is whether automated systems should be dedicated or shared, that is, whether the hardware in a system should be managed and used solely by criminal justice agencies. The alternative is to share hardware with other government agencies so that an information system might at one moment process criminal justice information and later process the state payroll, for example. Some criminal justice administrators favor the dedicated system to best assure the security of the system and its constant availability to criminal justice. Mainly because of cost factors, most administrators favor shared systems so that excess capacity can be used for other government services. Technical experts agree that information can be adequately secure in a shared system; criminal justice records can be properly segregated and protected.

Early drafts of the LEAA regulations required dedication, but this requirement does not appear currently. LEAA considers it a state or local prerogative to decide whether, and how, a system will be shared.

CHAPTER II. SPECIFIC ISSUES CONCERNING PRIVACY PROGRAM DEVELOPMENT.

Within the context of competing interests and fair information practices, specific issues of "privacy" or the confidentiality, of criminal justice information can be addressed.

Privacy Costs.

The costs of implementing confidentiality and security requirements in criminal justice information is an important factor. "Privacy" costs should be differentiated from those occasioned by a properly managed information system, and varying costs and associated with differing degrees of confidentiality and security should be appreciated.

The cost of establishing a properly managed information system should not be attributed to "privacy" needs. Most of the fair information practices discussed in Chapter I had less to do with privacy than with the integrity of the data system itself. Accurate and complete information should not be characterized as a privacy cost since any information system should strive to provide valid information to those who use it. Important information should be protected from unauthorized access or alteration, so the requirement of systems security cannot be appropriately characterized as a "privacy" cost. It is true that a poorly designed or managed information system cannot adequately protect information confidentiality or be responsive to privacy concerns. Nevertheless, the basic costs necessary to provide an adequate information system should not be confused with the additional costs that might be attributed specifically to privacy constraints.

A variety of options for confidentiality and security measures depend upon the degree of privacy protection desired. "Half a loaf is better than none," and system managers should be expected to supply estimates of the range of costs associated with various privacy and security options.

State Regulatory Authority.

Title 28, Part 20, suggests that a state level authority be established to provide uniformity with respect to policy and procedures for access to criminal justice information. Unless such an agency has the authority to require compliance with its rules and regulations as contrasted with an advisory role, adherence will depend upon voluntary action. Experience in the past suggests that a voluntary approach will prove unsatisfactory, given the number of collecting and reporting entities and their variant procedures.

A subsidiary question is whether access rules should apply only to a central repository or to local agencies as well. Confidentiality cannot be assured if local agencies provide information not available through the central repository. Accuracy of information may be impaired if an individual's record is disseminated by functionally separate agencies. Though information may be made conveniently available at the site of a local operating agency, there should be no dissemination until a check with the central repository has updated the file.

Privacy and Security Council.

The NAC has recommended that a council be established to provide evaluation and monitoring of the policy and procedures in the state. Such an agency also can provide an "ombudsmen" role, receiving complaints from individuals who believe their own privacy may be inadequately protected, or from those who do not believe that there is sufficient access to information. Is there need both for a state regulatory authority and a privacy council? There may be a tendency for the regulatory authority to become oriented toward the needs of the criminal justice system, though to some extent this depends upon the membership composition of the agency, and its role. It is possible that the "watchdog" function of a council could be accomplished by other governmental or public interest agencies, and each state may have other options available to it.

Relevance of Public Records Laws.

Many states have provisions that make certain records of official actions open to the public. The post-Watergate era has seen an increase in these laws to make more visible the operations of government. The quest for open government, however, need not mean that personal information concerning those with whom government deals should also be public. The state's open record laws should be examined to determine their scope and purpose in terms of criminal justice information.

Three questions are important: (1) Does the fact that a record is initially public require that it remain open to everyone indefinitely? (2) Does the marshalling into a single file of a series of separate public record transactions require that the resulting file itself be open to the public? (3) Are exceptions for criminal justice appropriate?

The sealing or destruction of, or limitation of access to, public records is accepted practice. In almost every state juvenile justice records are protected. In other cases, access limitations may be imposed when the interest served by the open record is outweighed by other pertinent interests. The passage of time may justify closing a record, or the occurrence of a subsequent event. The mere fact that a record is initially public does not mean that it must remain so indefinitely.

The aggregation of a series of public record transactions into a single file is a separate problem. Because government resources were used to prepare a dossier does not of itself mean that citizens should have access to it. Reports and analyses prepared for government executives are not public simply because they were prepared at government expense. To argue that because the aggregate is merely a collection of public transactions there is no need to restrict access, misses the point about dossiers. It is the very marshalling of separate and discrete transactions into a single file that can change the nature and potential fo the resulting information.

A more practical question is: What good does it do to restrict access to the compilation if the source records are public? Any citizen could himself compile the information by examining the separate public records, and to restrict the compilation might encourage "black market" information.

But the cost and inconvenience may often deter one from compiling a dossier. Imagine the burden of examining the chronological booking sheets at the various precinct police stations in a medium size city to determine whether a certain individual has ever been arrested. Only the most compelling circumstances would encourage such an undertaking, and a policy ought not be formulated based upon an exceptional case. As to the "black market" problem, of course improper or illegal conduct is always a threat. Criminal and civil liability for "black market" information may be a sufficient deterrent, but certainly it is unsound to argue that an interest ought not to be protected because wrongdoers may violate it.

Finally, consideration should be given to whether the state's open record law contemplates criminal justice information. Some laws have been on the books for years, and were passed without specific consideration of applicability to criminal justice records. In other instances, privacy concerns may not have been considered in making certain records public, and the scope and purpose of relevant laws should be assessed to determine whether amendment is advisable.

Regulation of Dissemination.

What presumption will apply to any question of access to criminal justice information? Will criminal justice information be considered open to the public, or not? This question addresses the balance of interest between the individual and society, and should be determined before any of the subsequent specific questions are considered. Two important consequences flow from settling the question. First, policy analysts have a starting point for addressing specific questions; particular criminal justice information will be presumptively open, or closed, to the public unless there can be shown contrary law or superior interest. Second, if the presumption is that criminal justice information is public, the open record becomes part of the penalty to be assessed against an offender; a burden in addition to whatever other sentence is imposed.

A tenet of our society is that one is considered innocent until he has, by due process of law, been proven guilty; it would be consistent to restrict access to arrest and non-conviction records. Since the stigma of a criminal record may prevent employment, which is necessary for rehabilitation, a persuasive argument can be made for a presumption of confidentiality even for conviction data.

On the other hand, society has an interest in protecting itself from criminals, and this militates in behalf of open criminal records. In such case each member of society makes his own judgment about the weight of a criminal record in decisions whether to employ or otherwise associate with another.

Rather than to apply the same presumption to all criminal justice information, an alternative is to apply a presumption of confidentiality to arrest records, non-conviction and intelligence and investigative information, but the contrary presumption to conviction data. That seems to be an implication of the LEAA regulations, and is worth considering.

Arrest Information.

Title 28 restricts public access to arrest records when there has been no disposition for more than a year, unless the data subject is in active process in the criminal justice system or there is authority for the dissemination in a statute, regulation, executive or court order. This restriction is consistent with the presumption of innocence, and denies any probative value to arrest information outside the criminal justice system.

It is frequently urged that simple arrest records ought to be available for pre-employment screening in sensitive positions or for elective office. It may be difficult to decide what jobs are "sensitive", and what information is actually relevant to such jobs. In any event, the important question is not the purpose of the inquiry but the probative value of the information itself. An arrest record merely indicates that charges have been asserted by a particular arresting officer, and can include allegations based upon reasonable mistake. Whatever the reason, if the state has not followed an arrest by prosecution there is good reason to limit access to stale arrest records.

It is sometimes argued that because an arrest is an historic fact, that the record of that fact should be public information. That argument begs the question, however, since the basic choice is to decide what records of historic fact will be public.

Non-Conviction Data.

When an arrest has been followed by officially recorded dismissal of charges, or a judge or jury has determined the accused is not guilty, then a stronger argument can be made for limiting access to such data. The simple arrest appears as an unchallenged assertion of suspicion, whereas non-conviction indicates an official determination that the suspicion is insufficient to support prosecution or criminal guilt. In that light, non-conviction data may have less value for screening purposes than the arrest record itself.

It is often argued that when non-conviction results from "technical" legal defects that have nothing to do with guilt in fact, the non-conviction data should be available to the public. This argument appears to be unsound for several reasons. First, guilt in law is the concern of the criminal justice system, and the due process that has shielded one from conviction should not then be used as a sword to open access to information of questionable value. Second, it is often impossible to determine from a record the precise reason for non-conviction, so all such records might be opened because some may have resulted from "technical" defects. Further, to permit the dissemination of non-conviction information may have the effect of denying one the full benefit of non-conviction since the risk of being negatively affected by a "criminal record," even though it indicates non-conviction, is a real one.

Investigative and Intelligence Information.

Perhaps the strongest case can be made for the strict confidentiality of I&I information, which frequently contains unsupported allegations or unverified information, as well as information of a most personal nature which may not be relevant to specific criminal conduct. The individual wants this kind of information kept confidential, if it is kept at all. The criminal justice system refuses public access to I&I information because disclosure may destroy any value it may have.

Conviction Information.

The question is whether the fact of conviction will be available to the public indefinitely. Society wants access to conviction data for a variety of justifiable reasons. The offender wants to regain status in society, and easily accessible conviction information will be an impairment to him. One option for the state is to restrict access to conviction data if an individual has no further involvement with the criminal justice system for some specified period of time. If such an option is desired, the subsidiary questions are: (1) what constitutes "involvement", (2) what period of non-involvement is reasonable, and (3) to what sorts of convictions should dissemination restrictions apply?

Involvement could mean an arrest whether or not it results in conviction, or it could be defined as conviction for a subsequent offense.

An arrest without subsequent conviction ought not to be considered "involvement" since a mistaken or unfounded arrest would serve to keep a criminal record open, and the legal immunities from civil liability do not help to deter careless arrests. It seems reasonable that involvement with the criminal justice system be defined as conviction resulting from a prosecution begun or completed within a specified limitation period.

With respect to the time period for an access restriction to become operative, it is often suggested that for misdemeanors or felonies not involving violence, periods of from three to five years are reasonable; for serious felonies, six to ten years may be reasonable. 13/ Some research into recidivism indicates that repeat offenses after such periods of non-involvement are unusual. 14/

Misdemeanors and non-violent felonies are generally regarded as the most amenable to restricted access after periods of non-involvement. This has been prevalent recently with respect to convictions for marijuana use, or for "political crimes" connected with civil disobedience.

Arguments are made for closing conviction records even for crimes of violence with respect to effectuating rehabilatation programs. A difficult question arises if restrictions apply also to especially sensitive employment responsibilities, or where there may be exposure to the same risks involved in the previous conviction; access to conviction data in such circumstances might be appropriate even though the data might not be available for inquiries concerning other employment. The question is one of relevance; to what kinds of subsequent employment is a particular conviction relevant with respect to screening?

A commonly used example is conviction for molesting children; it can be urged that such convictions are relevant to any employment entailing close or supervisory relationships with children. On the other hand, such a conviction may be irrelevant to employment as a construction worker or a bank teller. The question of relevance is complicated by a lack of precise knowledge as to why people commit crimes in the first place, which of course makes it difficult to understand the situations in which there may be continued risk of harm.

These difficulties should not prevent a state from choosing to have access restrictions after some period of non-involvement; they relate to what exceptions there may be to such access restrictions. The approach of exception-by-job-responsibility may provide a reasonable balance between the interests of prospective employers and those of the data subject. The result in such case is not to keep a person's record of certain convictions open to all indefinitely, but rather to make it clear that those convictions will be accessible if the data subject chooses to pursue particular avenues of employment.

It is extremely difficult to handle relevance by statutory language or by regulation, since in the final analysis a subjective judgment must be exercised. The question then is, who should exercise that judgment? The Maryland program discussed in Chapter III, for example, establishes a procedure whereby such discretion to allow access is exercised by the Secretary of the Department of Public Safety.

Government vs. Private Sector Access.

It is often assumed without discussion that government should have access for non-criminal justice purposes to criminal justice information from which the private sector is excluded. The most prevalent non-criminal justice inquiry is for employment screening; government jobs are presumed to involve a public trust and important responsibilities, which probably accounts for the special access privilege. Those assumptions are worth examining.

Considerations of "public trust" may differ as between elective office and public jobs acquired through appointment or competition. With respect to the latter, the "public trust" may not be so important as the nature of the job to be performed. Is the job one that entails such risks as to justify an inquiry into criminal history? Would an inquiry for a similar private sector job be permitted? Of course many governmental jobs involve access to information that may endanger state security or entail responsibilities that pose a special risk to person or property. There are parallel responsibilities also in the private sector; in both sectors there are many jobs wherein no special risks are involved.

When risk is involved, government may be able to cope with it than a private enterprise that could be wiped out by an embezzlement, for instance, that would be a relatively insignificant loss in a government operating budget. Suffice it to say that it is probably more valid to make judgments about job sensitivity based upon the nature of the job itself rather than whether the employer is a governmental or private entity.

A related question concerns access by licensing or regulatory agencies. Frequently private sector employment may require a license granted to those of "good moral character"; such a phrase may be interpreted as permitting inquiry into criminal history. Though of course such inquiries would be appropriate with respect to many licensed enterprises, some examples cause doubt as to whether the legislature gave serious thought to the question, especially where "good moral character" is required for license as a dog groomer, for instance. Though the LEAA regulations accept a "good moral character" provision as sufficient authorization for access to simple arrest or non-conviction records, state licensing regulations should be examined to assure that criminal justice information access is appropriate to the licensed function.

A final aspect of the government vs. private sector access question involves the role of private security services. The last decade especially has seen tremendous growth in the private security industry in the United States. Partially because limited governmental resources do not provide adequate security coverage, and because of the often specialized needs of the business world for investigative and security service, private security has grown to the point where conservative estimates are that those employees outnumber all of Federal, state and local law enforcement personnel perhaps by a factor of two or more. The recent increase of terrorist threats against industrial leaders has accentuated the growth of private security. The question is how to deal with the private security industry for purposes of criminal justice information access. Is it to be classified as law enforcement, or the private sector, or in some special category?

The definition of a criminal justice agency in Title 28 excludes the private sector since law enforcement is defined as a governmental function. LEAA took this position after lengthy and careful consideration of the issue. One reason may be the matter of accountability, that is, a governmental agency is subject to some degree of monitoring and accountability on behalf of the public, whereas this may not be the case in the private sector.

This matter should be addressed so that it is clear whether a state may choose to give private security access to criminal justice information under special circumstances and in accord with prescribed procedures. The NAC has prepared an extensive report on the private security industry, and that can be consulted. 15/

Access By Data Subject.

There is little reason to question the right of an individual to inspect a record pertaining to himself; he knows what has been his involvement and can check the accuracy and completeness of information. A valid objection can be made to inspection of investigative or intelligence information, however, since the very purpose for which such information is maintained could be vitiated if the data subject were to examine his files.

Right To Challenge.

The right of a data subject to inspect his file is of little consequence if he cannot request that incorrect or incomplete data be corrected or updated. Procedures to validate the challenge can protect against improper assertions. A right to challenge by an administrative procedure to be completed in timely fashion, with agency review in the event there is dispute over the challenge, would be reasonable. If a record is not chagned in accord with the request, perhaps the objection could be noted in the record with a brief explanatory statement supplied by the data subject.

Judicial Review of Challenged Information.

Many states have general provisions for judicial review of administrative decisions; these may or may not include challenges to criminal records. Though additional judicial burdens should be avoided, there is insufficient evidence at present to indicate that judicial review would pose a significant added burden. Criminal justice wants information to be accurate and complete, so there is little reason to anticipate disagreements that could not be resolved in the agency review.

Purging or Sealing.

Purging contemplates the complete removal of a record from information systems, either through destruction of the record or by return to the data subject. Sealing preserves the record though it is removed from the active files of the system, and thus access is prevented or sharply limited. The principal distinction between the two techniques is clear: purged information may never be officially recalled; sealed information may be made available in prescribed circumstances.

If information is no longer of any value to criminal justice or to the public, then it ought to be removed from the information system in the interest of cost and to protect the individual who might be harmed if the information should be disclosed. If arrest or non-conviction information has no probative value as a matter of law, then the information might well be purged, either by destruction or by return to the data subject. The latter technique may be more useful to the individual with respect to non-conviction records as a way to protect himself should information about his previous encounter with the system turn up in the future. For instance, suppose that an individual had been arrested by mistake and charges against him were accordingly dropped; later, the fact of the arrest comes to public light because an account of it is found in a newspaper morgue. The data subject will be in a better position to clear his name if he has the information in his possession.

It is more difficult to make an argument in behalf of purging conviction information during a data subject's lifetime, even though sealing might be appropriate. For instance, if a previous offender has no further encounters with criminal justice for a prescribed period of time, it may be the policy to limit access to the record. In the event of further involvement with criminal justice after the limitation period, however, then perhaps it would appropriate for that prior information to be made available.

If information is sealed it can be reopened, but if purged, it is lost. The subject of purging is such a sensitive issue to criminal justice personnel that it might be more reasonable to consider sealing, with differing reopening procedures for special circumstances. Purging may nevertheless be appropriate for convictions for matters that have been "decriminalized," such as alcohol or drug use, or "political" offenses.

An administrative question is whether sealing or purging should occur automatically or be triggered at the request of the data subject.

Since sealing removes information from active files, that could occur automatically pursuant to routine information audit and review procedures. It is reasonable that purging be requested by the data subject when he is entitled to do so, especially in instances when purging is accomplished by return of the records. Because purging probably would occur only after some appreciable length of time, finding the data subject may pose a burden which can be alleviated by requiring him to come forward. If purging is accomplished by destruction of records, then that procedure could be automatically triggered by periodic information system reviews, though the data subject might be unaware that his file was purged.

If sealing or purging is adopted, be sure that all record-holders comply. For instance, in one state where criminal records can be purged by court order, the court record itself, which displays the purged information, is public.

Removal of Disqualifications.

When the purpose of sealing or purging is to remove the onus of the criminal record, it is consistent also to remove disqualifications associated with the record.

Right To State Non-Existence of a Record.

The right to disavow a criminal history further implements procedures to seal or purge information and remove disqualifications. Thus, if one is asked if he ever committed an offense that has been purged, he would be entitled to answer, "No." A provision might prohibit questions concerning information that has been sealed or purged, but the right to deny the record goes a step further.

Researcher Access.

When information not referable to an identified individual is requested for research or statistical purposes, of course privacy cannot be impaired. The academic and research community make persuasive arguments, however, for the need to obtain information which is referenced to identifiable individuals. The researcher may need to aggregate data from a variety of sources with respect to a particular individual and therefore all such information must be identifiable. Longitudinal studies that track a particular individual over a period of time require identifiable information.

The need for such information is generally recognized; it has been specifically recommended by the Privacy Protection Study Commission and is permitted by LEAA regulations. Part 22 of Title 28 CFR, deals specifically with statistics and research, and describes procedures whereby privacy interest can be reasonably protected while research access is not unreasonably impaired. Confidentiality ought not to be easily defeated under the guise of research, and the policy and procedures of Part 22 appear to be adequate. NCJISS has issued a pamphlet discussing the implementation of Part 22.

Accuracy and Completeness.

Apart from "privacy" interests, useful information should be accurate and complete. The practical problem is how to assure faithful and timely reporting of dispositions and official transactions in the criminal justice process. The LEAA regulations regard 90 days as a reasonable time within which to report dispositions, and any information system ought to be able to comply.

Civil Remedies.

The issue is whether a data subject will be provided with special civil remedies for the violation of information regulations. The common law in most states already provides remedies in defamation or invasion of privacy for dissemination of inaccurate or incomplete information, which will probably not apply to denial of the data subject's own access rights or when the confidentiality of information has been breached. A right is of little practical value if there is no remedy for its violations; the Compendium can be consulted for examples of remedies.

Criminal Penalties.

The question is whether to assess criminal penalties instead of, or in addition to, any civil remedies available. Criminal penalties can be considered when employees intentionally and purposefully violate information management policy and regulations. Administrative penalties such as loss of job or transfer of duty are options for dealing with intentional violation or habitual negligence, though fines or incarceration can be the "teeth" that emphasize the importance of observing information management procedures. Again, the Compendium can be consulted for examples.

Separation of Files.

A requirement that intelligence and investigatory information be stored and maintained separately from criminal history record information seems to be a principle that can be accepted without debate. Frequently I&I information is speculative, conjectural, based upon subjective evaluation, unverified, yet very sensitive. Though I&I information may be useful, certainly Watergate and its aftermath have provided a multitude of examples of spiteful, erroneous or groundless information collected and maintained for purposes not in the general interests of government or society. The utility of I&I information to criminal justice may be defeated by unauthorized access; it can be at least embarrassing and perhaps ruinous to the data subject. The segregation of I&I information is usually the practice in law enforcement, and it is often suggested that I&I ought not to be put into automated systems.

Regulation of Intelligence Collection.

This issue goes directly to the question of privacy, that is, what and how information is collected for intelligence purposes. The most outrageous intrusions into one's privacy are protected by laws prohibiting electronic eavesdropping or illegal searches. The main issue of intelligence collection deals with the extent to which criminal justice agencies may have access to non-criminal justice information. Aspects of this question, beyond the scope of this report, have been dealt with in the report of the Privacy Protection Study Commission, cited earlier.

Regulation of Intelligence Dissemination.

Given the nature of intelligence information, it is difficult ever to make a case for the dissemination of such information beyond authorized law enforcement agencies. In particular disclosure of investigative or intelligence information would appear to be particularly questionable for employment licensing or similar non-law enforcement purposes in light of the frequently unverified status of the data.

Exchange of intelligence information within the law enforcement community is an issue of some sensitivity. Law enforcement officials are hesitant to disseminate such information outside their own agency, and when they do it is usually only to other officials with whom they are cooperating, and often in such cases the information is maintained in a manual file the notes of the officer who has gathered the information may be meaningful only to himself or someone else generally familiar with the file.

Security.

As previously stated, this report is not concerned with the techniques of security, but mainly with the need to establish the policy to provide security. Technical source documents will be helpful here. 16/

Transaction Logs.

Whether a system is manual or automated, the integrity and confidentiality of data can be enhanced if transaction logs record instances of access to files and identify the information that may have been added or disseminated. A transaction log can permit monitoring of files without the need to examine the raw data within the file. Apart from privacy and with respect to information management, the maintenance of transaction logs is a worthwhile practice.

Training of Employees.

An appropriate understanding of the policy and procedures to protest the confidentiality and security of information is necessary on the part of any personnel with access to information. Any information system manager should see to it that his employees are appropriately trained; statutory training requirements emphasize the need for formal programs and may help in securing the necessary funds to provide adequate training.

Listing of Information Systems.

A requirement of the Privacy Act of 1974, is that all Federal agencies must provide notice of personal information systems, describe the nature of the system, the kind of information it contains, and the procedures by which an individual may inquire about a file pertaining to himself. Though few states have such a statutory mandate, this is probably because the average person knows that criminal justice agencies keep files.

CHAPTER III. EXAMPLES OF STATE PROGRAMS FOR CONFIDENTIALITY AND SECURITY.

In connection with the survey of state legislation, four states were queried with respect to the process they employed in developing their program. These states, Colorado, Illinois, Maryland and Washington, are presented not as models for programs so much as examples of how a program was put together. Though this report discusses the substantive policy options for information confidentiality, the procedure for developing and implementing such a program requires careful thought and planning as well.

It is not suggested that these examples exhaust the ways in which a program can be "packaged". Each state has its own administrative, social and political environment that dictates variations in how best to proceed. Nevertheless, there are commonalities in process, and the sharing of experiences may result in new ideas.

At the conclusion of this Chapter there are some ideas about process that are worth considering during the planning and implementation of a program for criminal justice information confidentiality.

COLORADO

Colorado Criminal Justice System.

Colorado has two state level law enforcement agencies, the State Highway Patrol and the Colorado Bureau of Investigation. The Highway Patrol, situated within the state's Department of Highways, is responsible for patrolling state roads, the enforcement of traffic laws and providing support in emergency situations at the direction of the Governor. The CBI operates crime laboratories, an investigation division that provides technical assistance to local law enforcement agencies, and it maintains the identification bureau and criminal information center for the state. Established in 1973 in the Department of Local Affairs, CBI also has responsibility for the investigation of organized crime activities that may cross jurisdictional lines within the state.

The Chief Justice of the Supreme Court of Colorado has superintending control over all the courts in the state with the exception of municipal courts and the Court of Denver County. The State Court Administrator, who reports to the chief justice, is responsible for the management and administration of the courts. There are 22 district courts of general jurisdiction, and the 63 counties each have a court of limited jurisdiction, dealing with misdemeanors, the issuance of warrants, the setting of bail, etc. The County Court of Denver functions both as a city and a county court, and there are a number of other municipal courts throughout the state that are not part of the state judicial system.

The state has a unified correctional system encompassing maximum and minimum security institutions, prison camps and other facilities and services. Probation services are under the jurisdiction of the district and county courts.

Criminal Justice Information System.

In the early '70s the state began the development of automated criminal justice information systems. It experimented with a criminal history record system, and began an offender-based tracking system as part of a comprehensive data system for criminal justice. The state court system is developing a judicial management information system, and a management information system for the department of corrections is being developed as well. One judicial district has a prosecution management information system.

41

The privacy and security plan for Colorado contemplates that the arresting authority will forward fingerprints to the CBI together with the charges, and a criminal justice number will be assigned to the charged individual by the CBI at that time. The tracking process begins at that initial entry point; district attorneys are expected to report dispositions with respect to the charges which are also assigned numbers by the CBI, but the criminal justice number is the principal identifier for all subsequent processing in the system.

Development of the State's Privacy Program.

In 1973, the SPA established a Criminal Justice Information Advisory Committee to assist in the development of the state's criminal justice information system. The Committee was comprised mainly of law enforcement representatives, and it functioned informally to provide ongoing advice to the SPA staff. A Statistical Analysis Center (SAC) is located within the SPA.

In 1975, stimulated by the initial regulations issued by LEAA in March of that year, the SPA developed a general criminal justice information privacy and security plan which was reviewed by the Advisory Committee. The plan was submitted to LEAA in March, 1976, and included a detailed series of 41 milestones for task performance in connection with development of the privacy and security program; these are set forth as Figure 2, beginning at page 38 hereof. The SPA held back on dissemination requirements policy in expectation of revised LEAA regulations. The dissemination package was completed in June, 1976, subsequent to the issuance by LEAA of the revised regulations.

The Governor and other state and local officials had expressed some displeasure with what was perceived as Federal intervention into state matters because of the LEAA regulations; the requirements for dedicated systems were a particular bone of contention. The news media also reacted sharply to the dissemination restrictions in the first LEAA regulations. These concerns were considerably mollified by the revised regulations.

At the time the plan was submitted, Colorado had a public records law which was unclear with respect to its application to criminal justice information. It seemed to be the general practice of the CBI not to disseminate criminal justice information outside the system, though such information may have been available from local law enforcement agencies.

In September, 1976, the Governor established a separate Special Task Force on Access to Criminal Records, to develop the confidentiality policy called for by the plan. The membership of the Task Force was much broader than that of the Advisory Committee, and included representatives not only from state and local criminal justice agencies, but also from business, news media, the ACLU, private security, public interest groups and general local government. The Task Force held three public meetings to gather views on the subject of access to criminal records.

The Task Force drafted legislation amending the public records act so as to include criminal justice information, to authorize a central repository (the CBI) and to require criminal justice agencies to report their official actions to the repository. Upon submitting the draft to the Governor in January, 1973, the work of the Task Force was finished, and it disbanded. The Advisory Committee of the SPA continues to function in a monitoring role, providing advice and assistance in addressing implementation requirements.

The legislative proposal submitted by the Task Force to the Colorado legislature during its 1977 session was essentially an open record bill meeting the requirements of the LEAA regulations. The question of criminal justice information confidentiality did not seem to be of particular interest to the state legislature, though the House committee with jurisdiction over the bill did hold extensive hearings. The House imposed dissemination restrictions consistent with the SEARCH standards in Technical Report #13, closing non-criminal justice access to misdemeanor information after five years of non-involvement, and to felony information after seven years. It also provided that arrest information (without disposition in two years,) and non-conviction information, would be released only to criminal justice agencies. The Colorado Senate accepted most of the House amendments, and added a provision for automatic sealing of records after non-involvement with criminal justice for five years for misdemeanors and seven years for felonies. The effect was to provide substantially more confidentiality to criminal justice information than had been recommended by the Task Force.

The state law also has an interesting discretionary sealing provision which permits the data subject to apply to court for the sealing of specific criminal justice information. If the court finds

> "that the harm to privacy of the person in interest or dangers of unwarranted adverse consequences outweigh the public interest in retaining the records, the court may order such records, or any part thereof except basic identification information, to be sealed. If the court finds that neither sealing of the records nor maintaining of the records nor maintaining of the records unsealed by the agency would serve the ends of justice, the court may enter an appropriate order limiting access to such records."

The Act further provides that when records have been sealed or access limited, the data subject may deny the existence of the official actions covered by the order. (There is not a counterpart right of denial with respect to the automatic five and seven year limitation provisions, however.) Further, the law prohibits "employers, educational institutions, state and local government agencies from requiring an applicant to disclose any information contained in sealed records". It also provides that an applicant may not be denied a job solely on the basis that he refused to disclose the existence of a sealed record.

The legislation gives to the custodian of intelligence and investigative information the discretion to deny access "on the ground that the disclosure would be contrary to public interest."

Significant Issues.

In the development of the privacy and security plan, there was initial opposition from local law enforcement agencies to the notion of a central repository. Some of this opposition apparently resulted from dissatisfaction with the operation of the experimental computerized criminal history system; also there was some doubt expressed whether the state could adequately maintain an identification section. The local agencies were assured that they would have an input with respect to central repository policies and procedures. Many locals realized that they might not have the resources to maintain an adequate record system, and to do so would incur cost duplication. Local agencies are encouraged to maintain backup records, however, if they so choose. These factors together served to minimize concern about the central repository.

The central repository maintains fingerprints, missing and wanted persons information, criminal histories and uniform crime report data in automated files. Intelligence information is maintained at the central repository, though it is not automated.

Limitations on dissemination to non-criminal justice agencies was vigorously opposed by private security agencies, credit investigators, etc., and though they were apparently persuasive with respect to the Task Force position, the legislature did provide limitations as previously noted.

Local law enforcement agencies opposed the maintenance of a dissemination log, and did not like the requirement to query the central respository before disseminating information, and the legislation does not include these items. The users agreement provided by the CBI to those with access to the central repository does require the maintenance cf dissemination logs, however.

The judiciary was uncomfortable with the notion of closing access to court records since in many instances this is the only contact that the public has with its court system. The Supreme Court did not, however, take any position on the legislation though a representative of the State Court Administrator's office was fully involved in the Task Force effort. The public record law allows the Court Administrator and the CBI jointly to develop access rules with respect to judicial files.

Some Remaining Problems.

The disposition reporting process has yet to be thoroughly developed. There is question with respect to how municipal ordinance violations should be treated. Such violations are included within the definition of official actions covered by the public record law, and the amendments to require any "law enforcement, correctional, and judicial entity, agency, or facility" to furnish information to the CPI central repository. A significant aspect of this will be the treatment of the municipal courts. The Advisory Committee, CBI and the State Court Administrator are working to develop adequate reporting procedures.

Assuring accuracy and completeness is recognized as a problem. It may be two or three years before the court information system is thoroughly effective in the reporting process; local law enforcement agencies and prosecutors must be depended upon to accurately report their actions

The legislation does not define "non-involvement" and this may be a problem in interpreting that provision. It is not clear, therefore, whether arrest, conviction or something else may constitute involvement with criminal justice.

Because of limitations on access to conviction records and the provisions for sealing of records, Colorado might face a problem of "black market" information. Whether there is such a problem, and its dimensions, of course will not become evident for a few years yet.

Words From the Wise . . . .

Task Force members interviewed in connection with this survey seem to be pleased with the procedure used to develop their criminal justice access recommendations. Special emphasis was given to the broad representation of the Task Force, the utility of the public hearings for gathering views, and the supportive role of the SPA staff in drafting, etc. There was a general feeling, however, that there should have been contacts with the legislature much earlier. Though a member of the legislature was on the Task Force, there was no steady liaison with legislative leadership to prepare the way for Task Force recommendations. As a result, the legislature placed more limitations on access than had been recommended, though the Task Force did not anticipate that possibility.

CY 1976

Month & Task No.	Tasks	Responsible Agency	COLORADO Reference Page*
June			
1.	Coordinate privacy and security procedures between CBI and other criminal justice information systems.	CBI	2-4
2.	Revise the "Exchange of Computerized Criminal Histories agreement" to be more explicit and cover all exchange of criminal history record information.	CBI	4-4
3.	Establish a specific list of locations where an individual may request access to his criminal history record.	CBI	7-2
4.	Rewrite and expand instructions on access and review including standardized form for challenges and distribute to law enforcement agencies.	CBI	7-2
5.	Develop and distribute material for public consumption to Colorado Criminal justice agencies and make readily available for police distribution.	CBI	7-2
July			
6.	Strengthen the CSR by filling the vacant I.D. unit supervisor position.	CBI	1-6
September			
7.	Prepare model operations procedure pertaining to completeness and accuracy of information and query before dissemination.	CBI	3-2 & 3-3
8.	Complete the disposition reporting system design to integrate the court and corrections dispositions into the computerized criminal history.	CBI	3-8
9.	Modify existing record challenge procedures to include the use of a standardized form which identifies the specific entry being challenged, the reason and supporting documentation.	CBI	7-3

* REFERS TO PAGE IN PRIVACY PLAN DOCUMENT

10.	Develop and place into operations, internal CBI procedures for receiving challenges and conducting the administrative review.	CBI	7-4
11.	Develop and implement administrative appeal procedures involving the Attorney General as the responsible agency.	DCJ	7-4 & 7-5
12.	Prepare and disseminate policy regarding criminal justice agencies access, use and dissemination of criminal history record information.	CBI	4-4
October			
13.	Have a fully operational computerized criminal history.	CBI	2-2
14.	Develop and disseminate a booklet to criminal justice personnel on CHRI security responsibilities and obligations.	CBI	6-10
15.	Establish systematic audit procedures in court system.	Court	5-1 & 5-2
16.	Establish procedures for processing and reporting dispositions on arrests that are processed through municipal court.	CBI	2-3
17.	Commence the disposition reporting system in an operational mode supported by the necessary agreements, operational manuals and instructions.	CBI	3-8 & 3-9
18.	Establish systematic audit procedures in corrections systems.	Div. of Corr. Services	5-1 & 5-2
19.	Establish, implement and promulgate procedures for correcting erroneous records and for identifying and notifying agencies who have received these erroneous records.	CBI	7-5
December			
20.	Require that all terminal operators meet minimum security checks and receive training on the confidentiality of CHRI.	CBI	6-9
21.	Develop and implement specific security instructions to operators of the Judicial Department and Correctional Service Division Information Systems.	JD/CSD	6-10

CY 1977

Month & Task No.		Responsible Agency	Reference Page
January			
22.	Support the Query Before Dissemination Rule before disseminating criminal history record information.	CBI	3-10 & 3-11
23.	Establish policy and procedures regarding Query Before Dissemination Rule supported by user agreements between CBI and criminal justice agencies.	CBI	3-11
March			
24.	Complete the disposition reporting system for municipal court dispositions.	CBI	3-9
June			
25.	Prepare and pursue an Executive Order or legislation specifically designating CBI as the central state repository and operate the computerized criminal history.	Dept. of Local Affairs	2-1 & 2-2
26.	Prepare and pursue legislative action covering the submission of fingerprint cards.	Dept. of Local Affairs	2-2
27.	Prepare and pursue legislation specifically requiring disposition reporting.	Dept. of Local Affairs	3-5
28.	Commence the municipal court disposition reporting system supported with necessary agreements, operational manuals and instructions.	CBI	3-9
29.	Include in the systematic audit procedures the identification and inspection of criminal justice agencies who disseminate criminal history record information ensuring adherence to the regulations.	CBI	3-12

CY 19.. (Cont.)

Month & Task No. (June Cont.)	Tasks	Responsible Agency	Reference Page
30.	Prepare and pursue legislation relating to access and dissemination of criminal history information.	AG	4-3
31.	Establish, maintain and disseminate a list of non-criminal justice agencies authorized to receive criminal history record information.	CBI	4-5
32.	Review existing state statutes and ordinances, and, if necessary, draft legislation to allow local non-criminal justice agencies to use nonconviction criminal history record information for license and employment purposes.	AG/ Governor's Commission	4-7
December			
33.	Prepare and disseminate policies, procedures and forms covering contract (service) agencies.	CBI	4-8
34.	Prepare and disseminate policies, procedures and forms covering researchers.	CBI	4-9
35.	Prepare and pursue legislation providing for annual audit of all criminal justice agencies complete with sanctions.	AG	5-6 to 5-9
36.	Establish annual audit responsibility in Attorney General's office and create audit committee.	AG	5-6 & 5-7
37.	Establish operational delinquent disposition monitoring system.	CBI	5-4
38.	Establish audit trails systemwide to support systematic and annual audits.	CBI	5-5
39.	Establish dissemination logs systemwide.	CBI	5-6

CY 1977 (Cont.)

Month & Task No. (December Cont.)	Tasks	Responsible Agency	Reference Page
40.	Provide field staff to support systematic audit process.	CBI	5-2
41.	Establish systematic audit procedures systemwide.	CBI	5-1 & 5-2

51

ILLINOIS

Illinois Criminal Justice System.

The criminal justice system in Illinois is largely centralized in three entities: The Department of Law Enforcement, the State Court System, and the Department of Corrections.

The Department of Law Enforcement, headed by a Director who reports to the Governor, includes the State Fire Marshall, the State Police, the Division of Investigation, and the Bureau of Identification which operates the automated criminal justice information system. The Illinois Law Enforcement Commission (ILEC), which is the SPA, is established separately by statute in the Governor's Office.

The Bureau of Investigation is responsible for the investigation of organized crime, and provides technical assistance to local jurisdictions for the investigation of important crimes against the state; it maintains manual investigative and intelligence files not part of the criminal justice information system.

The State Police have responsibility for the enforcement of state traffic laws, the protection of the Governor and state property, and upon assignment by the Governor may deal with emergency and other special law enforcement situations. Direct law enforcement throughout the state is primarily the responsibility of several hundred local jurisdictions, including the 102 county sheriffs and many municipal and village police agencies.

Illinois has a unified court system established by the Constitution of 1970, which vests judicial oversight in the Supreme Court. There are 21 circuit courts of general jurisdiction, the largest being the Circuit Court of Cook County, while other circuits include from 2 to 12 counties. There are a variety of courts of limited jurisdiction in the state at the municipal level. Though the Constitution vests in the Supreme Court superintending control of all the state courts, a good deal of administrative authority has been delegated to the various circuit courts. The Administrative Office of Illinois Courts compiles and disseminates statistical information; the larger circuit courts also have court administrators. The Circuit Court of Cook County, responsible for about 60% of all judicial business in the state, is probably the largest trial court of general jurisdiction in the country.

The Department of Corrections has responsibility for state correctional institutions. Probation and parole services are under the jurisdiction of the various chief circuit judges.

Criminal Justice Information System.

Illinois is developing a Comprehensive Data System (CDS) that, in accord with the current state plan, includes capabilities for law enforcement and corrections agencies. At present there is no plan for a statewide court information system, though the State Court Administrator is coordinating development of such a plan.

The state's Law Enforcement Agency Data System (LEADS) maintains such on-line files as wanted persons and stolen articles, and accesses computerized criminal histories (CCH) maintained by the Bureau of Identification, and computerized files maintained by the Secretary of State. LEADS also interfaces with the National Law Enforcement Telecommunications System (NLETS) and the F.B.I.'s National Crime Information Center (NCIC). Underway now is the development of a Corrections Management Information System that supports the LEAA funded OBTS and OBSCIS. The CDS contemplates regional information systems in a network with LEADS.

Illinois began a centralized criminal information system with the passage in 1931 of the Criminal Identification Act which established a central repository that today is housed in the Bureau of Identification, within the Department of Law Enforcement. (Ill.R.S. Ch. 38, Sec. 206-7) That Act requires law enforcement agencies to report arrests and dispositions to the central repository. It also includes "privacy" measures by allowing records from the central repository to be disseminated only to peace officers for the administration of the criminal law. There also are provisions for dissemination of records to specified agencies and others pursuant to statute, ordinances or orders "as may be necessary in the identification of persons suspected or accused of crime and in their trial for offenses after being in prison or for prior offenses." In the case of Kolb v. O'Conner, 142 N.E.2d 815 (1957) the statute was held applicable only to the central repository and not to local criminal justice agencies. As a result, though information dissemination from the repository has been regulated, the practices of local law enforcement agencies have varied widely.

Development of the State's Privacy Program.

In 1972 the Department of Law Enforcement prepared an action plan for the development of a statewide criminal justice information system. In 1974, two advisory committees to the SPA were established to develop comprehensive policies for the criminal justice information system. These committees each reported their recommendations in 1974.

One committee, the CJIS Policy Review Advisory Committee, was comprised mainly of citizen representatives and academicians. The recommendation of this committee was a proposal for comprehensive legislation governing the collection, use and dissemination of criminal justice information. The proposal was far-reaching, and incorporated many of the standards of SEARCH Technical Report #13, including provisions for sealing and purging of conviction data. This legislative proposal was not acted upon by ILEC.

The other advisory group, a Users Planning Committee, was comprised, as the name implies, of representatives of criminal justice agencies. The recommendations of this committee were largely accepted by ILEC and are now published as the Standards for Criminal Justice Information Systems that must be observed by any agency receiving funding from ILEC for information system development. These comprehensive standards relate to all aspects of information system development and operation. With respect to dissemination regulation, the standards require expungement of information indicating arrest without conviction (or proceedings terminated in favor of the accused). As to other criminal justice information, dissemination is permitted on a "need to know and right to know" basis. The standards emphasize the maintenance of accurate information, and permit data subject review and challenge.

In the Fall of 1975, subsequent to the issuance by LEAA of its initial privacy and security regulations, the Governor designated the SPA staff as the mechanism to coordinate implementation of a state plan for the confidentiality of criminal justice information. Letters from the SPA to the State's Attorneys, the Department of Law Enforcement, the Attorney General, the State Court Administrator and the Department of Corrections, asked for reports with respect to their information systems. The courts regard their records as public, so the Illinois plan was prepared by the SPA staff mainly with assistance from the Departments of Law Enforcement and Corrections.

In March, 1976, shortly before LEAA's revised regulations were issued, the Illinois plan was submitted; a revision was submitted by ILEC in June, 1976, to respond to the LEAA changes.

In November, 1977, the Governor, by Executive Order, established the seven-member Criminal Justice Information Council, with the mandate to consider confidentiality and security requirements for criminal justice information. The Council is authorized "to issue regulations, guidelines and procedures which insure the privacy and security of criminal history record information consistent with state and federal laws . . . ." The Council is the final appeal body with respect to individual challenges to criminal histories, and it audits the procedures of the central repository.

Individual Review and Challenge.

A significant aspect of the Illinois program is its emphasis of data subject access to files, with rights of review, challenge and appeal. The SPA has taken steps to publicize these access rights; included here at page 47 as Exhibit 1 is a brochure published by ILEC that informs citizens of their rights of record review and challenge. After two years' experience with this provision, the Department of Law Enforcement indicates that the procedure has been quite manageable. Over the last year, because of extension of access rights to incarcerated individuals, requests for review have increased by 270%. Despite this percentage increase, however, statistics for the review and appeal caseload are interesting. During a 24 month period the statistics are as follows: Of 647 individual requests for review, only 88 challenged the record; of these only three were not satisfied by the initial DLE response and requested agency review wherein two were satisfied. As of this time, the remaining case is on appeal to the Criminal Justice Information Council and has been scheduled for early 1978.

The time for response to a request for record review averaged about 23 days; the time for responding to a record challenge has averaged about 20 days, and an average of about 19 days was required to process the administrative review. These time spans are within the DLE regulations, and the procedure does not appear to have placed an undue burden upon the department, allaying the fears of many who predicted that review and challenge procedures would be an unmanageable burden. Further, there has not been a significant increase in process time during the last 12 month period, when the large increase in requests was received.

Some Remaining Problems.

Compliance with disposition reporting procedures still poses some problem, as in many other states, though Illinois reports good progress in improving this process.

In spite of policies and a few statutory provisions permitting sealing or purging of certain information, it appears that many agencies will not seal or purge except pursuant to a court order. Since the courts regard their records as public, whatever might be purged or sealed in agency records would be available from the court record. The resolution of this problem must await the development of a court information plan by the Administrative Office of Illinois Courts.

The mechanisms for operating a rational program to regulate information dissemination in Illinois are all present. The ILEC staff provides continuing coordination throughout the criminal justice system. The Department of Law Enforcement operates the central repository, which is the key to the statewide system for all of criminal justice. The Criminal Justice Information Council fulfills a "watchdog" role as well as being a forum for the development of policy.

ILLINOIS

how to beat a bum rap sheet

YOU HAVE A RIGHT TO SEE A COPY OF YOUR CRIMINAL HISTORY RECORD

- Beginning March 16, 1976
- The information in your record should be correct.
- If the information is not correct, you can have it changed.
- Review forms are available at your local police station.
- Read the instructions inside.

YOU HAVE A RIGHT TO SEE A COPY OF YOUR CRIMINAL HISTORY RECORD*

Beginning March 16, 1976, every person has the right to see and correct information that the police, courts, correctional, and other agencies maintain. Included in your record is a list of what you have been arrested for, the dates you were arrested and released, and other details about each case.

WHY BOTHER?

The main reason you should want to review your record is to make sure that the information in it is correct. You will also want to be sure that your record includes only legally maintained information. *A record with incorrect information could keep you from getting a State or Federal job, from joining a branch of the armed services, or from obtaining a license in any of a number of different professions.* Judges, military recruiters, and various authorized employers can examine your record and they may be influenced by what they see. So you want to be sure that your record tells the true story of what happened, with the correct dates and facts.

IS IT HARD TO DO?

No. Reviewing your record is a very simple matter. First you must identify yourself and submit the proper form. Then you can look at your record and correct any errors that you find.

**also known as a "rap sheet"*

IF YOUR CORRECTIONS ARE DENIED

If your corrections are denied, in whole or in part, the notice you receive will tell you when you can see a written explanation of the decision. Bring both your *Request for Access and Review* and your *Record Challenge* to this appointment.

If you are not satisfied with the explanation you are given, there are two things that you can do. First you can apply for an Administrative Review. Application forms for this procedure are available at your local police station. If you are still not satisfied with the results after the Administrative Review has been completed, then you may file an Administrative Appeal with the Illinois Criminal Justice Information Systems Council. The Council's decision will be final unless you choose to file a civil suit in a court of law.

FOR FURTHER INFORMATION:

Contact your local police or county sheriff's office.

WARNING

IT IS A VIOLATION OF FEDERAL LAW (42 U.S.C. § 3771) TO USE THESE PROCEDURES FOR ANY PURPOSE OTHER THAN THE INDIVIDUAL REVIEW OF A CRIMINAL HISTORY RECORD. ANY EMPLOYER WHO REQUIRES SUCH INFORMATION AS A CONDITION OF EMPLOYMENT WILL BE SUBJECT TO A $10,000 FINE. VIOLATIONS SHOULD BE REPORTED TO THE UNITED STATES ATTORNEY'S OFFICE AND TO THE ILLINOIS CRIMINAL JUSTICE INFORMATION SYSTEMS COUNCIL IMMEDIATELY.

Illinois Criminal Justice Information Systems Council
Illinois Law Enforcement Commission
120 South Riverside Plaza
Chicago, Illinois 60606

HOW TO SEE YOUR RECORD

1. IDENTIFY YOURSELF

Go to any police station or county sheriff's office in the state of Illinois between the hours of 8 A.M. and 4 P.M., Monday through Friday. Tell them that you want to see your criminal history record. You will be given a form to fill out called a *Request for Access and Review*. A copy will be yours to keep. You will have to show some form of positive identification such as a driver's license or birth certificate, and you will be fingerprinted. Your prints have to be compared with those in your file to make sure that no one claiming to be you sees your record.

A fee may be charged by the local law enforcement agency to cover the costs of processing your review. This fee will not be more than $10.

2. MAKE AN APPOINTMENT

Put your copy of your *Request for Access and Review* in a safe place. Within 6 weeks you will receive an appointment notice in the mail telling you that your record is available. If you cannot come at the appointed time, let them know within 25 days by telephoning or by returing the notice in the mail. You should write a date and time on the notice when you will be able to come to see your record.

3. BRING YOUR COPY

Be sure to bring your *Request for Access and Review* and some form of positive identification with you when you go to see your record. If you forget to bring your request form, you will not be able to see your record at that time. If you have lost this form, you will probably have to start over, at step (1).

If you have any official documents concerning your record, you should also bring them with you.

4. BRING YOUR ATTORNEY

You may bring your attorney when you go to review your record. In fact, if you want your attorney to review your criminal history record for you, he or she can complete this process once you have identified

5. INSPECT YOUR RECORD CAREFULLY

Read your record over very carefully. Make sure that the information about you is completely true. If you have any questions, ask the reviewing officer and he or she will be able to help you. If you ask for it, you will be given a list of the non-criminal justice agencies which have obtained copies of your record since March 16, 1976.

If there are any errors on your record, no matter how small, tell the reviewing officer about them immediately. For further instructions, see the next section called "IF THERE ARE ANY ERRORS."

If there are no errors on your record, you may be asked to sign a statement saying that your record is correct. Whether you choose to sign this statement or not, your review is now complete.

IF THERE ARE ANY ERRORS

6. REQUEST CORRECTIONS

If you find any errors, the reviewing officer will give you a form called a *Record Challenge*. List the correct information on this paper and explain in detail why these corrections should be made. A copy of your *Record Challenge* will be given to you to keep.

If you need a copy of your record, you can obtain one by asking the reviewing officer.

7. A DECISION WILL BE MADE

Within 6 weeks you will receive a notice in the mail. This notice will tell you whether your corrections were approved or denied.

If your corrections were approved, you should bring your *Request for Access and Review* and your *Record Challenge* forms to the police station and check to see that the corrections have been made properly. All the organizations which have received copies of your record since March 16, 1976 will be notified of these corrections.

At this time, you may be asked to sign a statement saying that your record is correct. Whether you choose to sign this statement or

MARYLAND

Maryland Criminal Justice System.

Maryland has a rather centralized criminal justice system, largely achieved in the early 1970s through the establishment of the Department of Public Safety and Correctional Services. That department, headed by a Secretary and two deputies, has general authority over the State Police, the Department of Corrections, and the Department of Probation and Parole.

The State Police, whose Superintendent reports to the Secretary of Public Safety, has responsibility for general law enforcement in the state as well as for the operation of the criminal justice information system. In addition to highway patrol functions, state police provide law enforcement services by contract to some of the municipal jurisdictions within the state.

The 23 counties and the City of Baltimore all have law enforcement agencies, as do a variety of smaller municipalities. Though each county has a sheriff, several of the largest counties also have a police department.

The Department of Correctional Services, headed by a Commissioner who reports to the Secretary of Public Safety, has jurisdiction over the state's institutional facilities, and through a jail inspector, monitors the operations and standards of jails under county or local authority.

The Department of Probation and Parole, whose Director reports to the Secretary of Public Safety, is responsible for all probation and parole services within the state. Regional offices of the Department directly supervise field services and cooperate with the courts regarding the operation of probation services.

The judicial system in Maryland itself became unified in the early '70s, and is arranged in four tiers. The District Courts, under the supervision of a Chief Judge, are courts of limited jurisdiction. The Circuit Courts, operating at the county level, are courts of general jurisdiction and are under the supervision of the Chief Circuit Judge. The Court of Special Appeals is an intermediate appellate court for criminal and civil matters. The Court of Appeals is the supreme court of the state; its Chief Judge has superintending control of the entire court system. The State Court Administrator, who is appointed by the Chief Judge of the Court of Appeals, has responsibilities for judicial planning, budgeting, education and information system development.

Criminal Justice Information System.

In 1968, the Maryland SPA began planning a comprehensive statewide criminal justice information system. The initial program, designated MILES (Maryland Interagency Law Enforcement System) was intended to serve the entire criminal justice system in the state, including the courts. During the ensuing decade the state has continued to develop its criminal justice information system including capabilities for such LEAA-supported programs as comprehensive criminal histories (CCH), offender based tracking system (OBTS) and an offender based state correctional information system (OBSCIS), all within the comprehensive data system (CDS). A statewide court information system is also being implemented. In the Fall of 1973, the SPA staff began a criminal justice information system master plan. The Information System Policy Committee, established by the SPA, provided policy guidance in the development of the master plan which was finally completed in early 1975.

Stimulated by needs identified in the master plan with respect to a privacy program, and by the issuance of the initial guidelines by LEAA in May, 1975, a Security and Privacy Sub-committee of the Information Systems Policy Committee was established with the responsibility to develop a privacy and security program and to prepare appropriate legislation and regulations.

In early 1976, the SPA completed a draft privacy and security plan responsive to the initial LEAA guidelines. When the revised guidelines were issued by LEAA in March, 1976, the Maryland plan was also revised to comport with the new minimum requirements. The basic framework of the plan was implemented through legislation signed into law by the Governor in May, 1976. The purpose of the legislation, knwon as The Criminal Justice Information System Act, is

> ". . . to create and maintain an accurate and efficient criminal justice information system in Maryland consistent with applicable federal law and regulations, the need of criminal justice agencies in the state for accurate and current criminal history records information, and the right of individuals to be free from improper and unwarranted intrusions into their privacy." (Art. 27, § 742)

In brief, the legislation established a central repository for criminal records to be operated within the Maryland State Police and under the supervision of the Secretary of Public Safety and Correctional Services. The statute provides that the Secretary and the Chief Judge of the Court of Appeals should promulgate rules and regulations to establish, operate and maintain the criminal justice information system. The law also established an Advisory Board to review and comment on such rules and regulations and the operation of the information system. The legislation gives the right of inspection and challenge to data subjects, and, with respect to dissemination of information, provides that a "criminal justice agency and the central repository may not disseminate criminal history record information except in accordance with applicable federal law and regulations."

Development of the State's Privacy Program.

As summarized above, the staff of the SPA had the task of drafting the criminal justice information plan with the advice of the Security and Privacy Subcommittee. The Subcommittee was comprised of members representing all branches of government as well as a cross-section of criminal justice agencies. The Subcommittee was chaired by the Secretary of the Department of Public Safety, and other members were the State Court Administrator, representatives from the state legislature, a mayor, a Governor's staff legislative officer, representatives from the State Police and the Department of Correctional Services, a local police chief and a county councilman. In addition to assisting the SPA staff with the development of the security and privacy plan, this subcommittee also assisted in the development of the legislative proposal, referred to earlier, that established the formal structure for the Maryland criminal justice information system. The Privacy and Security Subcommittee has ceased to exist since its task has been accomplished, though the Information System Policy Committee of the SPA continues in its advisory role regarding operation of the criminal justice information system.

The Criminal Justice Information Advisory Board, created by Article 27, Section 744, has as its principal responsibility to advise the Secretary of the Department of Public Safety and the Chief Judge of the Court of Appeals on matters pertaining to the development, operation and maintenance of the criminal justice information system.

The membership of the advisory board, appointed by the Governor except as otherwise indicated, is as follows: three representatives of the judicial branch appointed by the chief judge of the court of appeals; two representatives of the Maryland legislature, one appointed by the leader of each house; two executive officials from state, county or municipal police agencies; one executive official from a correctional services agency; two elected county officials; one elected municipal officer, one State's attorney; and one person from the general public. Serving in an ex officio capacity are the Executive Director of the SPA, the Secretary of the Department of Public Safety, and the Attorney General of Maryland.

The Advisory Board developed the dissemination policy which was approved by the Secretary of Public Safety and the Court of Appeals. Legislation was introduced during the 1977 session but was not enacted, and regulations pursuant to authority in the Criminal Justice Information System Act were promulgated.

Dissemination Policy.

The regulations, set out here as Exhibit 2 beginning on page were originally prepared as a legislative proposal. They were made available for comment at a public hearing, but there was no significant comment and the regulations are to become effective substantially in accord with the draft.

The regulations deal with criminal history record information, and are silent as to intelligence and investigative information. The central repository itself, however, will only store criminal histories and not "I and I" information. The significant aspects of Maryland dissemination policy are as follows:

1. Criminal justice agencies will receive from the central repository conviction and non-conviction information for the performance of their criminal justice function or for the purpose of hiring or retaining employees. Access to conviction or non-conviction information is also allowed to the Maryland Public Defender or any defense counsel of record, bail bondsmen and appropriate agencies for statistical and research purposes, or to agencies under contract with an agency authorized to receive the data.

2. A governmental non-criminal justice agency may receive criminal justice information for employment purposes. If the agency has licensing powers it may have criminal justice information for the purpose of performing its functions in accord with a statute, regulation or court order allowing access to specified information.

3. A private sector organization may not have access to conviction data for employment screening unless it has been specifically approved to receive such information by the Secretary of the Department of Public Safety, upon a showing that the nature of the job carries a risk of harm to the employer or the general public. A private sector organization may not have access to non-conviction data unless it is specifically provided for by statute, regulation or court order.

4. Only the central repository may disseminate information to authorized non-criminal justice agencies. Criminal justice agencies may share information among themselves after an inquiry to the central repository to update the file. Secondary dissemination of criminal justice information is prohibited; it can only be used for the specific purpose for which it was received and none other. The regulations also require the maintenance of dissemination logs, and the existence or non-existence of a criminal record is not to be divulged to anyone who is not authorized to receive the record itself.

The policy supported by these suggested regulations provide protection to the individual who has a criminal record while at the same time allowing public access for good cause shown. The Maryland approach of providing a procedure for specific private sector access approval by the Secretary of Public Safety is novel and interesting. The question of relevance of criminal justice information to any particular employment risk is difficult to resolve, and requires a case-by-case evaluation. Though the state legislation enacted in 1976 specifically provides for judicial review of a data subject's challenge and correction rights, judicial review of the secretary's decision regarding special private sector access is not contemplated. The Maryland experience in the future will be worth watching to determine the efficacy of this administrative procedure.

The Criminal Justice Information System Law establishes the right of a data subject to review and challenge criminal history record information in the central repository. On a challenge to information, the central repository will audit the record, and if the data subject's challenge is sustained the record will be corrected. The central repository also will send notice of the corrected information to any agency to whom it has disseminated incorrect information, and the receiving agency is required to correct whatever record it maintains. Administrative and judicial review are provided for.

A significant problem encountered in developing the Maryland program has more to do with the technicalities of information management than with confidentiality policy. The question was what standard to apply for determining whether information is "complete and accurate." A major difficulty was the relationship between charges noted at arrest or booking and the charges that the prosecutor would pursue. Police agencies wanted to track the specific charges made by the police officer. With little or no modification these police charges are the same as those that appear on the charging document at the District Court. Therefore, District Court charges and dispositions could be tracked against the original police charge. A difficulty arises when the defendant is bound over to the Circuit Court from the District Court or goes directly to the Circuit Court. In such case the prosecutor intervenes and typically charges are redefined and, therefore, are not directly traceable to the police charges. The District Court charges were selected as the entry point for tracking purposes; where the case is bound over to the Circuit Court the case is tracked back to the District Court case number but the prosecutor's Circuit Court charges become the new entry point for tracking charges and their disposition.

An implementation problem yet to be solved adequately deals with the query to the central repository before information is exchanged with other criminal justice agencies. Currently an unsatisfactory delay is often experienced in response from the central repository though hopefully as the system is perfected this difficulty will be alleviated. Perhaps, in the interim, local records may suffice in some circumstances, yet to be negotiated.

Issues For The Future.

In early 1978, the dissemination policy will be implemented, and wrinkles will be ironed out. It remains to be seen whether and how soon legislation will be sought to codify this policy; regulations can suffice except with respect to the imposition of criminal penalties. It will be well worth watching the Maryland experience with respect to the administrative procedure by which the Secretary of Public Safety approves private sector access for employment screening purposes. Maryland officials are optimistic regarding the workability of their scheme, and it may provide one solution to a very complex access question.

A Comment On Process.

Maryland officials credit their centralized criminal justice system as key in developing the privacy program. System fragmentation is a common obstacle to developing statewide information dissemination policy, especially with respect to disposition reporting procedures. In this respect, a court system may pose a particular problem if its various forums are uninvolved in program development or uncoordinated in approach. It should be noted that the Maryland judiciary was a full and active partner throughout the process, and continues to be involved in and responsible for the design and implementation of policy and procedure.

REVISED SECTION "749"

MARYLAND

749. DISSEMINATION OF CRIMINAL HISTORY RECORD INFORMATION*

(A) A CRIMINAL JUSTICE AGENCY AND THE CENTRAL REPOSITORY MAY NOT DISSEMINATE CRIMINAL HISTORY RECORD INFORMATION EXCEPT IN STRICT ACCORDANCE WITH THIS SECTION.

(B) SUBJECT TO THE PROVISIONS OF SUBSECTION (F) THE CENTRAL REPOSITORY AND A CRIMINAL JUSTICE AGENCY SHALL DISSEMINATE CRIMINAL HISTORY RECORD INFORMATION BE IT CONVICTION OR NON-CONVICTION CRIMINAL HISTORY RECORD INFORMATION, TO A CRIMINAL JUSTICE AGENCY UPON A REQUEST MADE IN ACCORDANCE WITH APPLICABLE RULES AND REGULATIONS ADOPTED BY THE SECRETARY OR THE COURT OF APPEALS. A CRIMINAL JUSTICE AGENCY MAY REQUEST SUCH INFORMATION FROM THE CENTRAL REPOSITORY OR ANOTHER CRIMINAL JUSTICE AGENCY ONLY IF IT HAS A NEED FOR THE INFORMATION:

(1) IN THE PERFORMANCE OF ITS FUNCTION AS A CRIMINAL JUSTICE AGENCY: OR

(2) FOR THE PURPOSE OF HIRING OR RETAINING ITS OWN EMPLOYEES AND AGENTS.

(C) SUBJECT TO THE PROVISIONS OF SUBSECTIONS (F) AND (G) AND EXCEPT AS OTHERWISE AUTHORIZED BY SUBSECTION (E), THE CENTRAL REPOSITORY MAY NOT DISSEMINATE TO A NONCRIMINAL JUSTICE FEDERAL, STATE, OR LOCAL GOVERNMENT AGENCY:

(1) CONVICTION CRIMINAL HISTORY RECORD INFORMATION UNLESS THE PERSON OR AGENCY TO WHOM THE INFORMATION IS TO BE DISSEMINATED IS EXPRESSLY AUTHORIZED BY STATUTE, ORDINANCE, EXECUTIVE ORDER, OR COURT RULE, DECISION, OR ORDER TO GRANT, DENY, SUSPEND, REVOKE, OR TERMINATE A LICENSE, EMPLOYMENT, OR OTHER RIGHT OR PRIVILEGE, AND THE STATUTE, ORDINANCE, ORDER OR RULE SPECIFIES THE EXISTENCE OR NON-EXISTENCE OF A PRIOR CONVICTION

---

*Originally drafted as an amendment to the Criminal Justice Information System Law, now to be implemented by regulation.

Exh. 2, cont'd.

OR OTHER CRIMINAL CONDUCT AS A CONDITION TO THE GRANT, DENIAL, SUSPENSION, REVOCATION, OR TERMINATION OF THE LICENSE, EMPLOYMENT, RIGHT, OR PRIVILEGE. REFERENCES TO "GOOD MORAL CHARACTER," "TRUSTWORTHINESS," OR OTHER LESS SPECIFIC TRAITS ARE SUFFICIENT TO AUTHORIZE DISSEMINATION WHERE THEY ARE DETERMINED BY THE COURTS TO BE INCLUSIVE OF CRIMINAL CONDUCT: AND

(2) NON-CONVICTION CRIMINAL HISTORY RECORD INFORMATION UNLESS THE PERSON OR AGENCY TO WHOM THE INFORMATION IS TO BE DISSEMINATED IS EXPRESSLY AUTHORIZED BY STATUTE, ORDINANCE, EXECUTIVE ORDER, COURT RULE, DECISION, OR ORDER TO GRANT, DENY, SUSPEND, REVOKE, OR TERMINATE A LICENSE, EMPLOYMENT, OR OTHER RIGHT OR PRIVILEGE, AND THE STATUTE, ORDINANCE, EXECUTIVE ORDER, OR COURT RULE, DECISION OR ORDER SPECIFIES ACCESS TO NON-CONVICTION RECORD INFORMATION IN CONSIDERATION OF THE DECISION TO GRANT, DENY, SUSPEND, REVOKE, OR TERMINATE A LICENSE, EMPLOYMENT, RIGHT, OR PRIVILEGE.

(D) SUBJECT TO THE PROVISIONS OF SUBSECTIONS (F) AND (G) AND EXCEPT AS OTHERWISE AUTHORIZED BY SUBSECTION (E), THE CENTRAL REPOSITORY MAY NOT DISSEMINATE TO A PRIVATE NON-GOVERNMENTAL EMPLOYER OR THE PRIVATE EMPLOYER'S DESIGNATED AGENT:

(1) CONVICTION CRIMINAL HISTORY RECORD INFORMATION UNLESS THE EMPLOYER DEMONSTRATES TO THE SECRETARY THAT THE ACTIVITIES OR DUTIES OF THE PROSPECTIVE EMPLOYEE OR EMPLOYEE FOR WHOM THE CONVICTION CRIMINAL HISTORY RECORD INFORMATION IS REQUESTED WOULD:

(a) BRING THE PROSPECTIVE EMPLOYEE OR EMPLOYEE INTO SUCH CLOSE AND SENSITIVE CONTACT WITH THE PUBLIC THAT THE USE OF THE INFORMATION IN HIRING, TRANSFER, OR PROMOTION OF THE EMPLOYEE WOULD SERVE TO PROTECT THE SAFETY OR BE IN THE BEST INTERESTS OF THE GENERAL PUBLIC: AND

(b) BRING THE PROSPECTIVE EMPLOYEE OR EMPLOYEE INTO SUCH CLOSE AND SENSITIVE CONTACT WITH THE EMPLOYER'S ENTERPRISE AS TO ENDANGER THE GOODWILL OR FISCAL WELL-BEING OF THE ENTERPRISE.

THE SECRETARY WILL ESTABLISH A PROCEDURE WHEREBY EMPLOYERS MAY PETITION FOR THE RIGHT TO BE GRANTED ACCESS TO CONVICTION CRIMINAL HISTORY RECORD INFORMATION CONSISTENT WITH SUBSECTIONS (a) AND (b) ABOVE. THE PETITION SHALL REQUIRE THE EMPLOYER TO LIST THE INSTANCES WHERE ACCESS IS DESIRED AND THE REASON FOR REQUESTING THE ACCESS CONSISTENT WITH THIS SUBSECTION. THE SECRETARY, WITH THE ADVICE OF THE ADVISORY BOARD, SHALL DEVELOP SPECIFIC CLASSES FOR WHICH ACCESS CONSISTENT WITH THIS SUBSECTION ARE TO BE PROVIDED AND SHALL MAINTAIN FOR EACH CLASS A LIST OF ALL EMPLOYERS WHO HAVE PETITIONED FOR AND BEEN GRANTED ACCESS.

(2) NON-CONVICTION CRIMINAL HISTORY RECORD INFORMATION UNLESS THE EMPLOYER IS EXPRESSLY AUTHORIZED BY STATUTE, ORDINANCE, EXECUTIVE ORDER, OR COURT RULE, ORDER, OR DECISION SPECIFYING THE RIGHT OF ACCESS TO NON-CONVICTION RECORD INFORMATION AND THE PURPOSE AND CONDITIONS FOR ACCESS.

(E) THE FOLLOWING NONCRIMINAL JUSTICE PERSONS AND AGENCIES MAY RECEIVE FROM THE CENTRAL REPOSITORY CONVICTION AND NON-CONVICTION CRIMINAL HISTORY RECORD INFORMATION FOR THE PURPOSE AND UNDER THE CONDITIONS STATED:

(1) THE DEPARTMENT OF PERSONNEL OR OTHER APPOINTING AUTHORITY OF THE FEDERAL, STATE OR LOCAL UNIT OF GOVERNMENT MAY RECEIVE SUCH INFORMATION FOR THE PURPOSE OF EMPLOYMENT SUITABILITY OR ELIGIBILITY FOR SECURITY CLEARANCES:

(2) THE MARYLAND PUBLIC DEFENDER OR ANY DEFENSE COUNSEL OF RECORD MAY RECEIVE SUCH INFORMATION FOR THE PURPOSE OF THE DEFENSE OF A CLIENT IN A PENDING CRIMINAL PROCEEDING;

(3) A BAIL BONDSMAN MAY RECEIVE SUCH INFORMATION RELATING TO A CLIENT, IF AUTHORIZED BY THE MARYLAND RULES;

(4) THE JUVENILE SERVICES ADMINISTRATION MAY RECEIVE SUCH INFORMATION FOR THE PURPOSES OF AN INVESTIGATION PURSUANT TO THE DISPOSITION OF A JUVENILE CASE;

(5) THE GOVERNOR'S COMMISSION ON LAW ENFORCEMENT AND THE ADMINISTRATION OF JUSTICE MAY RECEIVE SUCH INFORMATION FOR THE PURPOSES OF RESEARCH, EVALUATION, AND STATISTICAL ANALYSIS OF CRIMINAL ACTIVITY, AND THAT ANY STATISTICAL ANALYSES DERIVED FROM SUCH INFORMATION MAY NOT INCLUDE THE NAME OF ANY INDIVIDUAL OR ANY OTHER UNIQUE IDENTIFIERS RELATING TO THE INDIVIDUAL;

(6) A PERSON OR AGENCY ENGAGED IN LEGITIMATE RESEARCH, EVALUATION, OR STATISTICAL ANALYSIS ACTIVITIES MAY, PURSUANT TO AN AGREEMENT WITH THE SECRETARY OR THE CHIEF JUDGE OF THE COURT OF APPEALS, RECEIVE SUCH INFORMATION NECESSARY TO THESE ACTIVITIES, BUT SUCH INFORMATION MAY NOT INCLUDE THE NAME OF ANY INDIVIDUAL;

(7) A PERSON OR AGENCY UNDER CONTRACT WITH A CRIMINAL JUSTICE AGENCY TO PROVIDE SPECIFIC SERVICES REQUIRED BY THE CRIMINAL JUSTICE AGENCY TO PERFORM ANY OF ITS CRIMINAL JUSTICE FUNCTIONS MAY, PURSUANT TO AN AGREEMENT WITH THE SECRETARY, RECEIVE SUCH INFORMATION NECESSARY IN ORDER TO CARRY OUT ITS CONTRACT;

(F) A CRIMINAL JUSTICE AGENCY MAY NOT DISSEMINATE CRIMINAL HISTORY RECORD INFORMATION TO ANOTHER CRIMINAL JSUTICE AGENCY UNTIL THE DISSEMINATING AGENCY HAS REQUESTED AND RECEIVED FROM THE CENTRAL REPOSITORY VERIFICATION THAT THE INFORMATION TO BE DISSEMINATED IS COMPLETE, ACCURATE, AND CURRENT. THE CRIMINAL JUSTICE AGENCY OR THE CENTRAL REPOSITORY SHALL VERIFY THE IDENTITY OF THE CRIMINAL JUSTICE AGENCY TO WHOM THE DISSEMINATING

AGENCY INTENDS TO PROVIDE THE INFORMATION. THE CENTRAL REPOSITORY SHALL MAINTAIN A RECORD OR LOG OF THE REQUEST SHOWING THE DATE THE REQUEST WAS MADE, THE INFORMATION TO BE DISSEMINATED, THE CRIMINAL JUSTICE AGENCY RECEIVING THE INFORMATION, AND THE DATE OF THE DISSEMINATION. THIS SUBSECTION DOES NOT APPLY IF THE RECEIVING CRIMINAL JUSTICE AGENCY DEMONSTRATES TO A RESPONSIBLE OFFICIAL OF THE DISSEMINATING CRIMINAL JUSTICE AGENCY OR THE CENTRAL REPOSITORY THAT A DELAY IN THE RECEIPT OF INFORMATION FROM THE CENTRAL REPOSITORY WILL UNDULY IMPEDE NECESSARY ACTION BY THE REQUESTING CRIMINAL JUSTICE AGENCY OR WILL VIOLATE OR MATERIALLY IMPAIR A SUBSTANTIVE RIGHT OF THE PERSON ABOUT WHOM THE INFORMATION IS NEEDED. HOWEVER, THE DISSEMINATING AGENCY SHALL MAINTAIN A LOG OF EACH DISSEMINATION UNDER THESE CONDITIONS, SHOWING THE DATE OF DISSEMINATION, THE INFORMATION TO BE DISSEMINATED, THE CRIMINAL JUSTICE AGENCY TO WHOM IT WAS DISSEMINATED, AND THE DATE OF THE DISSEMINATION.

(G) ONLY THE CENTRAL REPOSITORY MAY DISSEMINATE CRIMINAL HISTORY RECORD INFORMATION TO A NON-CRIMINAL JUSTICE AGENCY OR INDIVIDUAL. THE CENTRAL REPOSITORY SHALL VERIFY THE IDENTITY OF THE AGENCY OR PERSON REQUESTING TO RECEIVE THE INFORMATION AND SHALL MAINTAIN A RECORD OR LOG OF THE REQUEST SHOWING THE DATE THE REQUEST WAS MADE, THE PURPOSE FOR WHICH THE REQUEST WAS MADE, THE INFORMATION TO BE DISSEMINATED, THE AGENCY OR PERSON RECEIVING THE INFORMATION AND THE DATE OF THE DISSEMINATION. THE CENTRAL REPOSITORY THROUGH AGREEMENT WITH ANOTHER CRIMINAL JUSTICE AGENCY MAY SPECIFY THE OTHER CRIMINAL JUSTICE AGENCY AS A LOCATION FROM WHICH A NON-CRIMINAL JUSTICE AGENCY OR INDIVIDUAL MAY INQUIRE TO THE CENTRAL REPOSITORY FOR THE PURPOSE OF RECEIVING CRIMINAL HISTORY RECORD INFORMATION. THE AGREEMENT MAY ALSO PROVIDE FOR THE CENTRAL REPOSITORY TO AUTHORIZE THE CRIMINAL JUSTICE AGENCY TO DISSEMINATE TO THE NON-CRIMINAL JUSTICE AGENCY APPROPRIATE CRIMINAL HISTORY RECORD INFORMATION MAINTAINED BY THE CRIMINAL JUSTICE AGENCY. UNDER

SUCH CIRCUMSTANCES THE DISSEMINATING CRIMINAL JUSTICE AGENCY SHALL MAINTAIN A LOG OF EACH DISSEMINATION, SHOWING THE DATE THE REQUEST WAS MADE, THE PURPOSE FOR WHICH THE REQUEST WAS MADE, THE INFORMATION TO BE DISSEMINATED, THE AGENCY OR PERSON RECEIVING THE INFORMATION, AND THE DATE OF THE DISSEMINATION. THE CENTRAL REPOSITORY SHALL MAINTAIN IN ITS LOG THE FACT THAT IT AUTHORIZED THE CRIMINAL JUSTICE AGENCY TO DISSEMINATE THE CRIMINAL HISTORY RECORD INFORMATION AND THE AGENCY OR INDIVIDUAL TO WHOM THE CRIMINAL HISTORY RECORD INFORMATION WAS DISSEMINATED.

(H) NO AGENCY OR INDIVIDUAL SHALL CONFIRM THE EXISTENCE OR NON-EXISTENCE OF CRIMINAL HISTORY RECORD INFORMATION TO ANY PERSON OR AGENCY THAT WOULD NOT BE ELIGIBLE TO RECEIVE THE INFORMATION ITSELF.

(I) ANY LOGS REQUIRED TO BE KEPT UNDER THIS SECTION SHALL BE MAINTAINED FOR AT LEAST THREE YEARS.

(J) THE USE OF CRIMINAL HISTORY RECORD INFORMATION BY AN AUTHORIZED AGENCY OR INDIVIDUAL IS LIMITED TO THE SPECIFIC PURPOSE OR PURPOSES STATED IN THIS SECTION AND MAY NOT BE DISSEMINATED FURTHER EXCEPT WITH SPECIFIC AUTHORIZATION.

E) ~~(K) IN ADDITION TO ANY OTHER REMEDY OR PENALTY AUTHORIZED BY LAW, ANY INDIVIDUAL OR AGENCY VIOLATING OR CAUSING A VIOLATION OF THE PROVISIONS OF THIS SECTION IS GUILTY OF A MISDEMEANOR, AND UPON CONVICTION, IS SUBJECT TO A FINE OF NOT MORE THAN $5,000 OR IMPRISONMENT FOR NOT MORE THAN SIX MONTHS OR BOTH FOR EACH VIOLATION. IF THE PERSON IS EMPLOYED OR LICENSED BY A STATE OR LOCAL GOVERNMENT AGENCY, A CONVICTION SHALL CONSTITUTE GOOD CAUSE TO TERMINATE HIS EMPLOYMENT OR TO REVOKE OR SUSPEND HIS LICENSE.~~

(K) IN ADDITION TO ANY OTHER REMEDY OR PENALTY AUTHORIZED BY

TION) LAW ANY INDIVIDUAL OR AGENCY DETERMINED BY THE SECRETARY TO BE IN VIOLATION

OR CAUSING TO BE IN VIOLATION THE PROVISIONS OF THIS SECTION SHALL CONSTITUTE GOOD CAUSE FOR THE SECRETARY TO TAKE THE NECESSARY STEPS TO ENFORCE COMPLIANCE INCLUDING REVOCATION OF ANY AGREEMENT BETWEEN THE AGENCY AND THE CENTRAL REPOSITORY AS WELL AS APPROPRIATE JUDICIAL OR ADMINISTRATIVE PROCEEDINGS TO ENFORCE COMPLIANCE.

(L) WHERE A REQUEST FOR THE DISSEMINATION OF CRIMINAL HISTORY RECORD INFORMATION IS MADE BY A CRIMINAL JUSTICE AGENCY FROM ANOTHER STATE DISSEMINATIONS WILL BE LIMITED TO THE PURPOSES FOR WHICH CRIMINAL HISTORY RECORD INFORMATION WILL BE DISSEMINATED TO CRIMINAL JUSTICE AGENCIES WITHIN THE STATE OF MARYLAND.

WASHINGTON STATE

Washington Criminal Justice System.

The Washington State Patrol enforces traffic laws on the state's highways, protects state property, and provides special law enforcement services in emergencies and at the Governor's direction. Law enforcement in the state is mainly attended to by the 39 county sheriffs; the cities of Seattle and Tacoma provide police services, but few other municipalities have significant law enforcement responsibilities. The state has few urban centers and the growing trend toward combined city/county law enforcement consolidation has emphasized the role of the sheriffs. The State Patrol operates a crime analysis unit, a central identification bureau and an organized crime intelligence division. The Patrol has responsibility for operating the state's central criminal justice information system.

Correctional services in the state are centralized in the Department of Social and Health Services, which includes adult corrections, the Board of Parole and the probation and parole services.

Though the state does not have a unified court system, the Supreme Court does have superintending control of the Superior Courts of the state, which operate at the county level and have general jurisdiction. District Courts are of limited jurisdiction and deal with misdemeanors, warrants, etc.

Criminal Justice Information System.

Washington is building a comprehensive state criminal justice information system, and at present central law enforcement information is computerized and accessed by more than a hundred terminals throughout the state. A correctional information system is being developed within the Department of Social and Health Services, and is designed to track adult felony offenders in institutional custody or under probation or parole supervision, and will provide management information services as well. A Superior Court Management Information System is in the developmental stage as well, and is intended to provide statewide judicial system information with respect to case status and process, dispositions and relevant caseload data.

In 1967, a criminal justice identification center was created within the State Patrol. In 1972, when the center became computerized, the legislature established it as the Central Identification Section (CIS) with authority to maintain identification and and criminal history records. Local law enforcement agencies were required to report arrests and provide CIS with fingerprints as the means for identifying files. The legislation also restricted dissemination of CIS records to criminal justice purposes only, and data subjects were given rights to review and challenge their records. These dissemination and access regulations did not apply to local law enforcement agencies, however.

Development of the State's Privacy Program.

In 1974, a bill was introduced in the Washington legislature to provide confidentiality restraints on state and local arrest records, but the bill never moved out of committee. Again in 1975, another bill was introduced, which would have prevented intelligence and investigative information from being placed in automated systems, imposed confidentiality constraints on arrest and conviction information, and would have given access and challenge rights to data subjects. There were hearings on the bill, but it was not enacted.

The issuance in 1975 of the initial LEAA regulations stimulated additional activity in the state of Washington, and in December, 1975, an Advisory Committee for Security and Privacy was established by the Governor. The Attorney General was chairman of the Committee, and it included representatives of criminal justice agencies at the state and local level, public interest groups, media and the state legislature.

By March, 1976, the Advisory Committee had prepared its initial recommendations which were widely circulated throughout the state for comment. The Committee proposal recommended restrictions on the dissemination of conviction records as well as arrest information; there were also recommendations for the inspection and correction of records, the maintenance of dissemination logs and procedures for the audit of criminal justice practices. A bill was introduced in the legislature which was the basis for the measure that ultimately was enacted in 1977.

The bill that passed the legislature was narrower than that proposed by the Advisory Committee. Because of the proposals in 1974 and 1975, previously mentioned, the legislature had some familiarity with issues relevant to confidentiality of criminal justice information, and hearings in the legislature emphasized concern about additional costs resulting from dissemination restrictions and the added burdens to criminal justice agencies from procedures to assure access and confidentiality.

Dissemination Policy.

The principle features of the Washington State Criminal Records Privacy Act are these:

1. The central repository must be queried for update before any criminal justice agency disseminates a record concerning gross misdemeanors or felonies. Some exceptions are provided; e.g., if time is of the essence and the repository cannot respond within the required time.

2. Conviction records may be disseminated with restriction, and there are no provisions for sealing or purging conviction data.

3. Criminal justice agencies may disseminate nonconviction data to other criminal justice agencies for purposes of criminal justice administration or for employment in the criminal justice system. Interestingly, the statute provides that criminal justice agencies may exchange information "without any obligation to ascertain the purpose for which the information is to be used by the agency making the inquiry."

4. Nonconviction data may be disseminated outside the criminal justice system if such access if specifically authorized by statute, orders or rules, or for research purposes, or pursuant to a contract to provide services to a criminal justice agency.

5. Dissemination logs must be maintained.

6. Nonconviction data may be deleted from records upon application by the data subject unless the charges result in deferred prosecution or other diversion, or the data subject has a prior felony conviction or subsequent arrest within two years.

7. The data subject has rights of review and challenge except for intelligence or investigative files. Nonconviction data may not be mechanically copied or reproduced.

8. The SPA has authority to administer the Act and to promulgate regulations for its implementation.

The legislation does not deal with dissemination of intelligence and investigative information, which is maintained by the intelligence unit separately from other criminal justice information in the Central Identification Section. While the data subject is denied access to such information under the legislation, the public records law, mentioned below, contains a conditional exemption of such information from its disclosure and copying provisions.

There is, however, a "reverse" effect from this legislation with respect to conviction data. The prior law regulating CIS did not permit dissemination of conviction data outside the criminal justice system; even though that restriction did not apply to local law enforcement agencies, some of them followed it anyway. The result of the new law is to relax the prohibition of release of conviction information by making such release discretionary but subject to disclosure dissemiation requirements. The legislature accepted this change because it closely parallelled LEAA regulations and was an acceptable compromise for the news media.

The Advisory Committee would have also restricted dissemination of conviction data if the data subject had no further conviction for seven years. The legislature accepted the presumption of confidentiality of nonconviction data, but applied the reverse presumption to conviction data, contrary to what had been prior policy in the state.

It is noteworthy that the SPA has authority to administer the Act and to adopt regulations. The SPA has promulgated regulations to spell out appropriate procedures under the law.

Other Laws Affecting Criminal Justice Information.

Public records law. The Washington State Open Government Act regulates campaign financing, lobbyist activities, reporting of financial affairs by elected officials, and public records. A portion of the policy declared in that legislation states:

> "That, mindful of the right of individuals to privacy and the desireability of the efficient administration of government, full access to information concerning the conduct of the government on every level must be assured as a fundamental and necessary precondition to the sound governance of a free society."

The presumption is that government agency records are public, and virtually any file, record or piece of information can be an agency record. With respect to criminal justice information, however, there is a conditional disclosure exemption for:

> "Specific intelligence information and specific investigative records compiled by investigative, law enforcement, and penology agencies, and state agencies vested with the responsibility to discipline members of any profession, the non-disclosure of which is essential to effective law enforcement or for the protection of any person's right to privacy."

A narrow interpretation of that exemption would exclude criminal histories, which would result in a conflict between this disclosure law and the CIS confidentiality requirement previously discussed. The new Act resolves this problem.

Amendment of the public records law could have obviated the need for a separate criminal justice records law, thus utilizing the Washington Public Disclosure Commission to oversee criminal justice information as well. Recognition of unique requirements for criminal justice resulted in a parallel but separate treatment of its information.

State Human Rights Commission Regulations.

The Washington State Human Rights Commission (HRC) exists for the purpose of protecting the disadvantaged, with special reference to minorities and the handicapped. The commission has promulgated regulations which deal with fair employment practices, two of which specifically relate to criminal justice.

Commission regulations declare it to be an unfair practice to make a pre-employment inquiry about a simple arrest record. It is also declared to be an unfair practice to refuse to hire someone solely on the basis of an arrest record, though law enforcement agencies are exempted from this regulation.

Further, HRC regulations declare it an unfair practice to refuse to hire someone simply because of a prior conviction unless the conviction is less than seven years old and it is relevant to specific qualifications for a job. The underlying policy for this regulation is somewhat in conflict with the dissemination of conviction data as permitted by the criminal justice records law. As noted previously in this report, however, such inconsistencies are not infrequent in any state's information regulations.

Issues For The Future.

In Washington, as in other jurisdictions, implementation of effective disposition reporting practices has yet to be completely developed. Cooperation of prosecutors and the courts is critical here, for reporting by law enforcement and corrections agencies is considered to be far more manageable at the moment.

One problem here, however, arises because by law CIS can be accessed only through provision of fingerprints. Many courts, especially those of limited jurisdiction, do not bother with fingerprints as a personal identifier. This difficulty has yet to be addressed.

Some Points On Process.

Chapter II considered the substantive policy issues to be confronted with respect to access regulations for criminal justice information. Based upon some observations of state experiences with the process for developing and implementing an information program, here are some ideas worth considering:

1. Establish a special task force or advisory group to develop or review the confidentiality program. The group may have an educational and advocacy role in the pursuit of legislation or regulation; a broad-based group including representatives from citizens groups, business, news media, state and local government criminal justice agencies, will have advantages in pursuasion. The group will need staff support for preparation of a program and to assure continuity in follow-through when the program is ready, so it ought to be attached to an important agency that has responsibility for the group and its work.

2. Examine the existing relevant laws or regulations that deal with access to criminal justice information, be they public record provisions or access authorization of regulatory or licensing agencies. Know what policies or inconsistencies are represented in the law.

3. Learn what are the current practices of the criminal justice system regarding access to information; they may already provide reasonable confidentiality but lack uniformity, or there may be gross inadequacies. In any event, the potential impact of access regulation should be appreciated.

4. Map carefully and well in advance, the process, issues, decision points and timetable for the program. Early agreement on such fundamentals as the presumptions regarding criminal justice access and the approach to government vs. private sector access will expedite the formulation of overall policy and procedures.

5. Establish good liaison with legislative leadership early in program development. It may be misleading to have representation from the legislature on the task force unless that person is interested in the program and will have responsibility for it when it reaches the legislature. It is important also that the Governor's legislative staff be kept abreast of the group's work.

6. Provide an opportunity for interested groups to be heard early in the process. The ACLU and human rights groups are generally active in behalf of confidentiality; news media and the business community frequently want broad access rights. Timely contact with such groups may avoid conflicts when legislation is under active consideration.

7. Build cooperation within the criminal justice system. It is important that state and local operating agencies see benefits for themselves by participating in the privacy program. If in exchange for faithful disposition reporting to the central repository, for instance, local agencies receive information helpful to them in the management of their own functions, their support will be more likely.

8. Do not be misled by exaggerated cost estimates for implementing a program. Though privacy is not free of cost, it probably can be achieved at a more reasonable expense than may be estimated by those who simply do not want to change the way in which they handle information.

The task of developing a comprehensive and rational program for criminal justice information regulation is formidable. It is hoped that this report has helped to provide a starting point and a structure for policy analysis, no matter how much or how little a state may choose to do in managing its criminal justice information system.

FOOTNOTES

1. Criminal Justice System, G.P.O. 1973-9-494-818; see Report of the National Advisory Commission on Criminal Justice Standards and Goals, generally Chapter 8.

2. P.L. 93-83, 42 U.S.C. 3701 et. seq.

3. A handbook published by Theorem Corporation, "How To Implement Privacy and Security," is a detailed document of procedures responsive to LEAA regulations, and may be obtained from the company at 1737 North 1st Street, Suite 590, San Jose, California 95112.

3. SGI stands for SEARCH Group, Inc., a private non-profit corporation dedicated to research and development in criminal justice information. SGI published Technical Report No. 13, "Standards for Security and Privacy of Criminal Justice Information," which contains useful discussion of suggested standards and policies for confidentiality and security of criminal justice information systems. SGI has also produced a glossary of criminal justice terms, and other publications dealing with criminal justice information technology. From time to time this report will refer to materials generated by SGI, many of which are available free to officials of state and local criminal justice. The address is 1620 35th Avenue, Suite 200, Sacramento, California 95822.

5. G.P.O. #1700-0016.

6. Personal Privacy in an Information Society, G.P.O. 052-003-0395-3.

7. For some guidance see the Theorem Handbook, n. 3; also National Bureau of Standards Technical Note 809, "Privacy and Security in Computer Systems," available from the G.P.O.

8. This report does not discuss technical compliance with Title 28 specifically. Useful information in that regard may be found in the Theorem and SEARCH publications cited at n. 3 and n. 4. LEAA, through SGI, conducted extensive workshops around the country to acquaint the criminal justice community with Title 28 implementation requirements, and literature in that regard is available from SGI.

9. 381 U.S. 479 (1965).

10. 96 Sup. Ct. 1155 (1976)

11. A discussion of the Federal case law appears in a paper by Paul Woodard, former SGI General Counsel, reprinted in the proceedings of the Third International SEARCH Symposium, May, 1976, available from SGI.

81

12. Some law enforcement administrators argue that there should be restrictions on dissemination of simple arrest information even within the criminal justice system itself, e.g., an officer should make his decision to arrest not based upon inquiry into prior history but because the circumstances at hand warrant an arrest.

13. SGI *Tech. Rept. No. 13*, Std. No. 18, suggests 5 years for misdemeanors and 7 years for felonies.

14. See, e.g., the article by Kitchener, Schmidt & Glaser, "How Persistent is Post-Prison Success," in March, 1977, issue of *Federal Probation*.

15. An additional resource is the report of a Forum on Criminal Justice Information Use sponsored by SGI. The Forum, held in 1977, considered private sector security access to CJI, and the report should be available soon from SGI.

16. See n. 4.

☆U.S. GOVERNMENT PRINTING OFFICE: 1978 281-380/4009 1-3

Other Publications of NCJISS Privacy and Security Staff

Privacy and Security of Criminal History Information: A Guide to Dissemination	(NCJ 40000)
Privacy and Security of Criminal History Information: A Guide to Record Review	(NCJ 48125)
Privacy and Security of Criminal History Information: A Guide to Administrative Security	(NCJ 49110)
Privacy and Security of Criminal History Information: A Guide to Audit	(to be released)
Privacy and Security of Criminal History Information: A Compendium of State Statutes	(NCJ 48981)
Privacy and Security of Criminal History Information: An Analysis of Privacy Issues	(NCJ)
Privacy and Security of Criminal History Information: A Summary of State Plans	(NCJ)
Privacy and Security Planning Instructions	(NCJ 34411)
Confidentiality of Research and Statistical Data	(NCJ 47049)
Confidentiality of Research and Statistical Data: A Compendium of State Legislation	(NCJ 44787)